How Does Mobility Fit Into the Internet Layering Scheme?

Organized by:
Wesley M. Eddy
NASA GRC / Verizon FNS

Moderated by:
Joseph Ishac
NASA GRC

Protocol Layering

- Keeps individual protocols simple
  - Different, complementary goals for each layer
  - Ease of implementation, deployment, upgrades
  - Solutions can be isolated to a single layer
    - Host Addressing, Routing, Fragmentation – L3
    - Data Ordering, Reliability, Port Multiplexing – L4

However ...
Not All Layer Roles are Well-Defined

- Many things can (and are) done in multiple places
    - Retransmission-based reliability:
      Done in both TCP and some physical links
        - Potentially causes problems for TCP
    - Security: could use TLS, IPsec, WEP, all, none
        - Computationally expensive to repeat at multiple layers

Original Stack Design

- In the early days, some features were either explicitly not included (security) or had not been thought of yet (mobility)
- It's not surprising that they didn't end up as tightly integrated into the layering scheme as things like routing, fragmentation, ordering, addressing of hosts/services, etc

Fundamental Restriction

- The layering interface is by no means verbose
- We give and take buffers between layers, with minimal status codes
  - There is no concept of fine-grained notifications between layers
    - Hello link-layer, this is real-time audio, please don't worry too much about reliability for my packets, I can not tolerate the delay or reordering

Host Mobility

- We can do this just about everywhere
  - And have multiple proposals for each layer and even in between layers
- Can layers cooperate to make it easier?
  - Mobile IP over Mobile ad-hoc protocols
  - Mobile SCTP over Mobile IP
  - Mobile aware TCP over Mobile IP
    - Allow TCP to re-estimate state for new paths

Competition to the Death, or Peaceful Coexistence?

- We have some host mobility schemes that can operate largely independent of each other
  - Mobile IP, HIP, Mobile SCTP, session layers, application layers
  - How many standards will Microsoft implement?
  - How many will my wristwatch be able to simultaneously support?
  - How many will providers deploy? support?

What is the Optimal / Optimum Solution?

- What is best for users?
  - Cheapest, easiest, wide-scale deployable, transparent, secure, etc
- Is there room for multiple host mobility architectures within a single mobile Internet?
- Should we rethink the layering interfaces?
  - Not just for mobility

Panelists

- We'll hear some opinions from:
  - Will Ivancic
  - Pekka Nikander
  - David Maltz

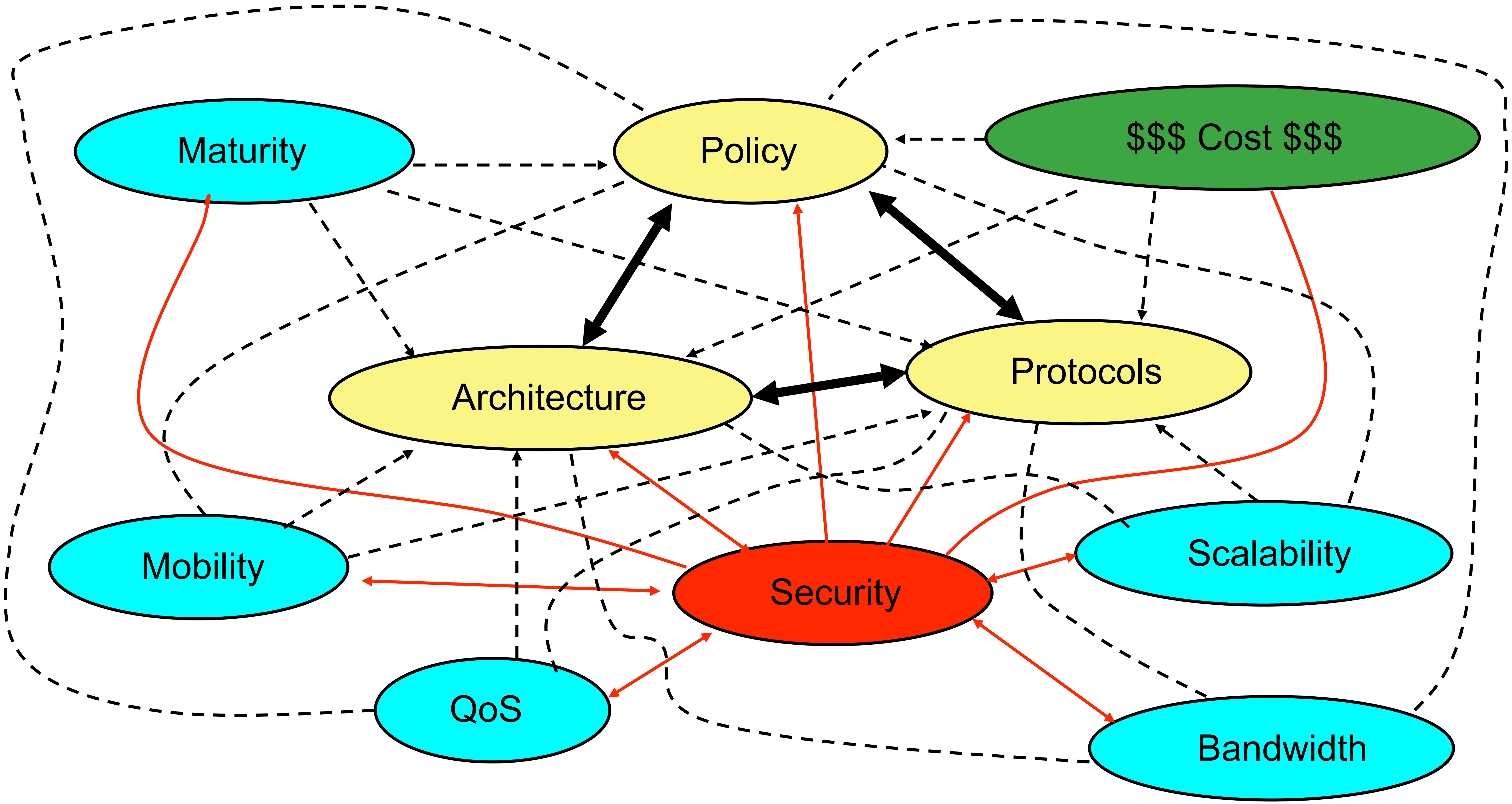
SYZYGY Engineering

Practical Considerations for Securely Deploying Mobility

Will Ivancic
NASA
Glenn Research Center
(216) 433-3494
wivancic@grc.nasa.gov

Network Design Triangle

SYZYGY Engineering



Design Issues

- Host and/or Network Mobility
- Security Policy
  - Corporate and/or Individual
- Scalability
- Handoff Speed
- Intranet or Internet
  - Own and/or Shared Infrastructure
    - May be and issue even within you own Organization
  - Crossing Autonomous Systems
- Multi-Homing
  - Multiple Radio Links
  - Varying Multi-homed link characteristics (e.g WiFi, Satellite, GPRS, Low-Rate VHF)

Mobile Networking Solutions

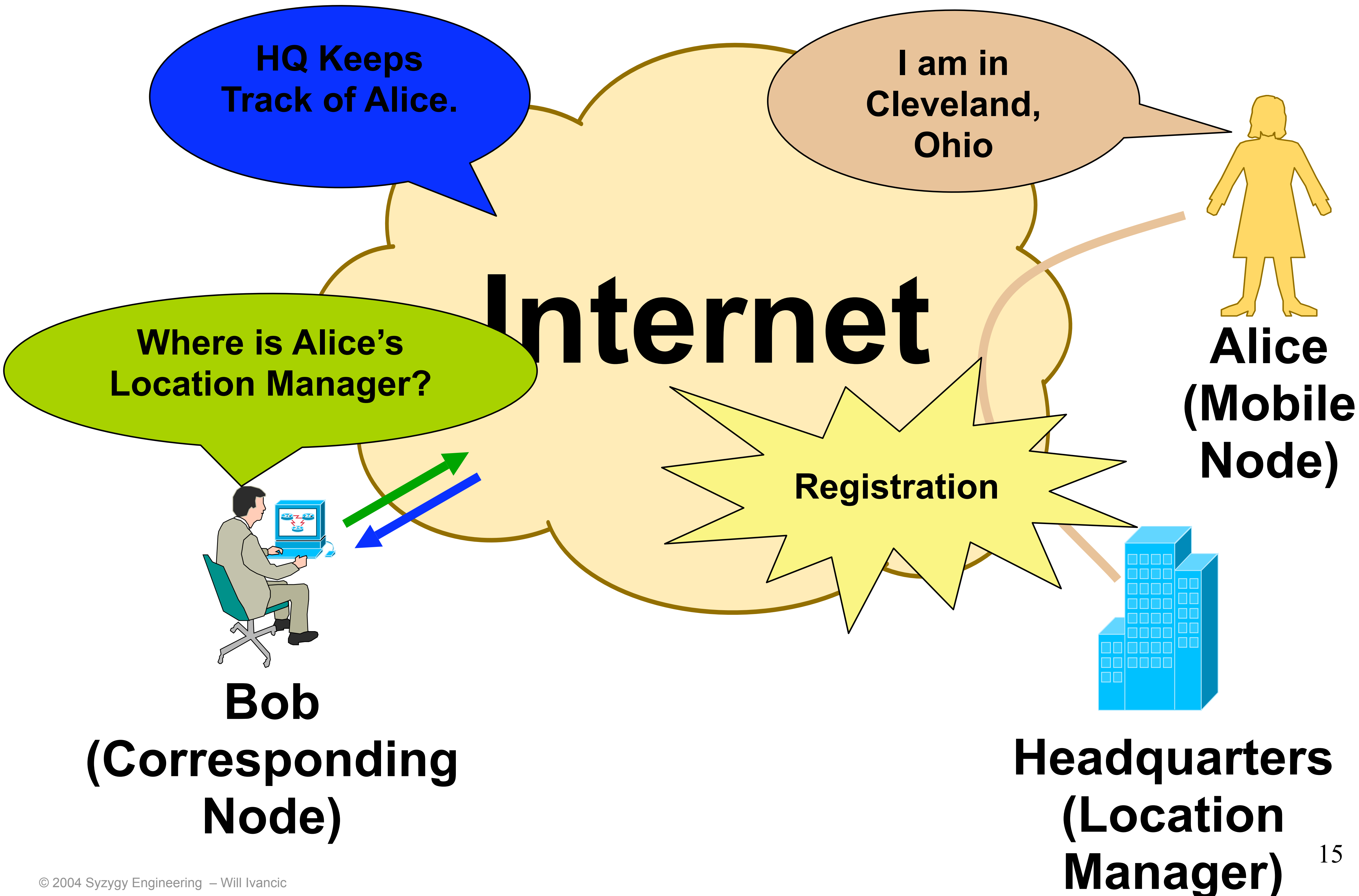
- Routing Protocols
  - ☺ Route Optimization
  - ☹ Convergence Time
  - ☹ Sharing Infrastructure – who owns the network?
- Mobile-IP
  - ☹ Route Optimization
  - ☺ Convergence Time
  - ☺ Sharing Infrastructure
  - ☺ Security – Relatively Easy to Secure
- Domain Name Servers
  - ☺ Route Optimization
  - ☹ Convergence Time
  - ☹ Reliability

Mobility at What Layer?

- Layer-2 (Radio Link)
  - – Fast and Efficient
  - – Proven Technology *within the same infrastructure*
    - Cellular Technology Handoffs
    - WiFi handoffs
- Layer-3 (Network Layer)
  - – Slower Handover between varying networks
  - – Layer-3 IP address provides identity
  - – Security Issues
    - Need to maintain address
- Layer-4 (Transport Layer)
  - – Research Area
  - – Identity not tied to layer-3 IP address
  - – Proposed Solutions
    - HIP – Host Identity Protocol
    - SCTP – Stream Control Transport Protocol

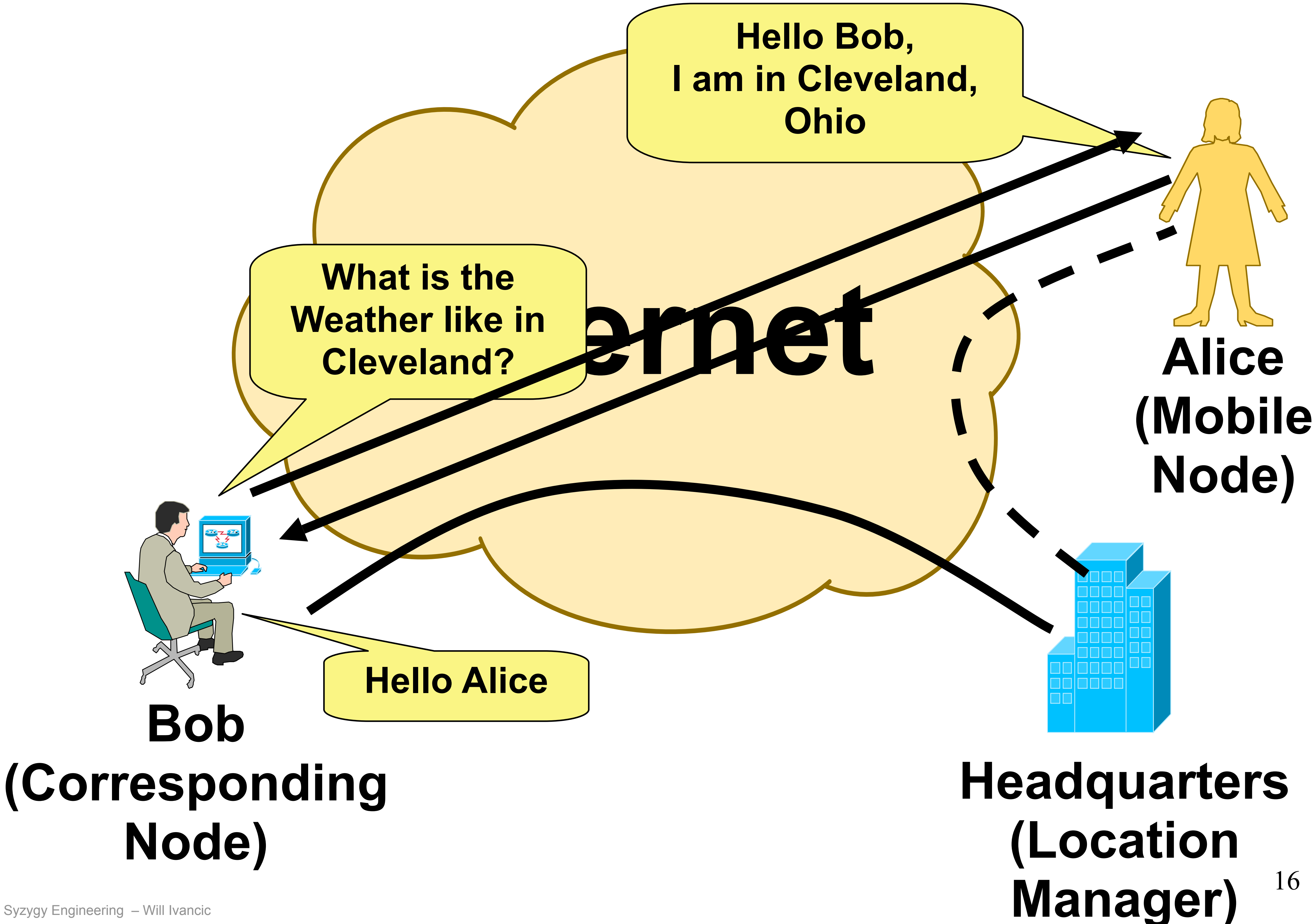
Location Identifier

SYZYGY Engineering

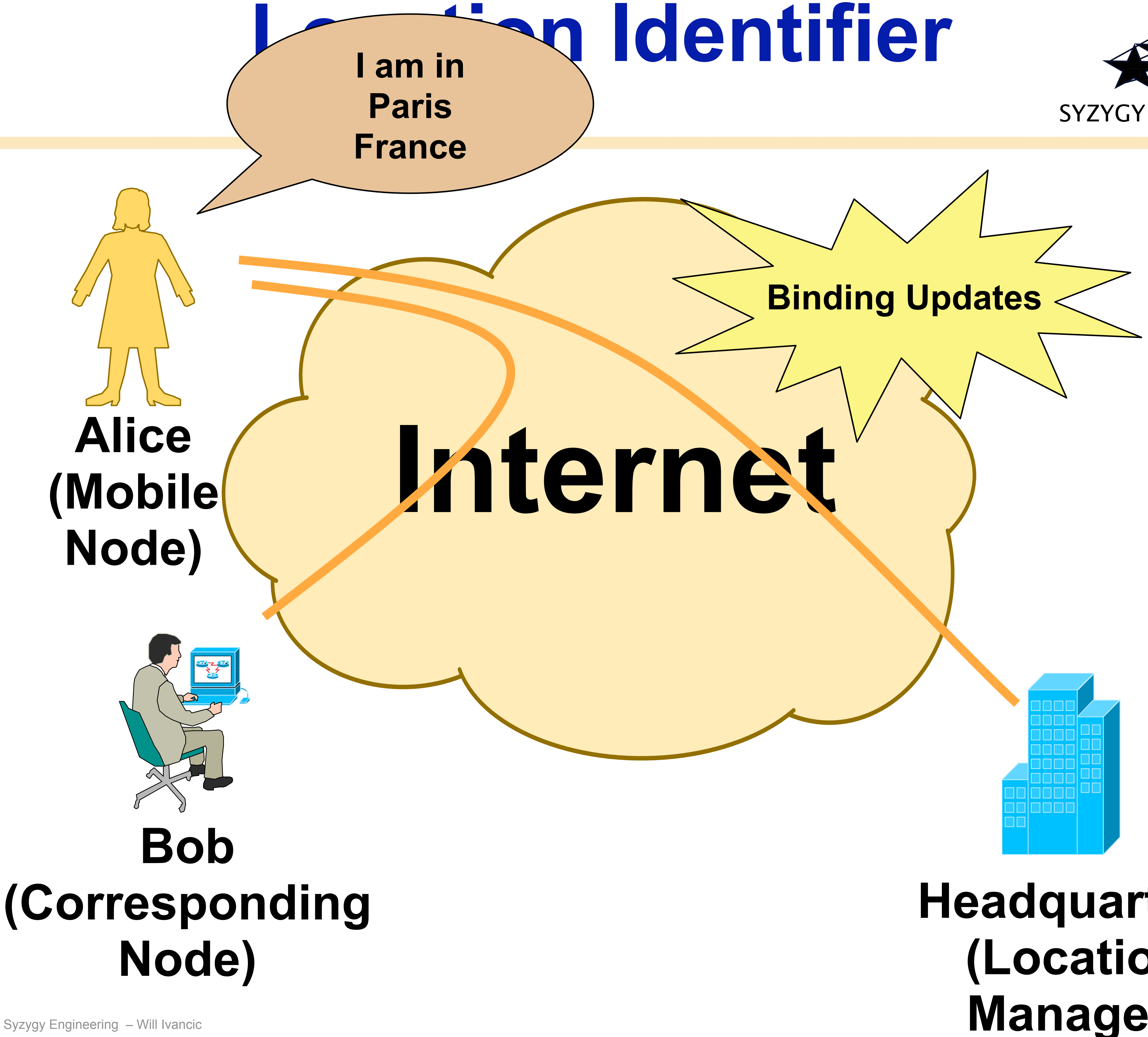


Location Identifier

SYZYGY Engineering



Location Identifier



I am in Paris France

Binding Updates

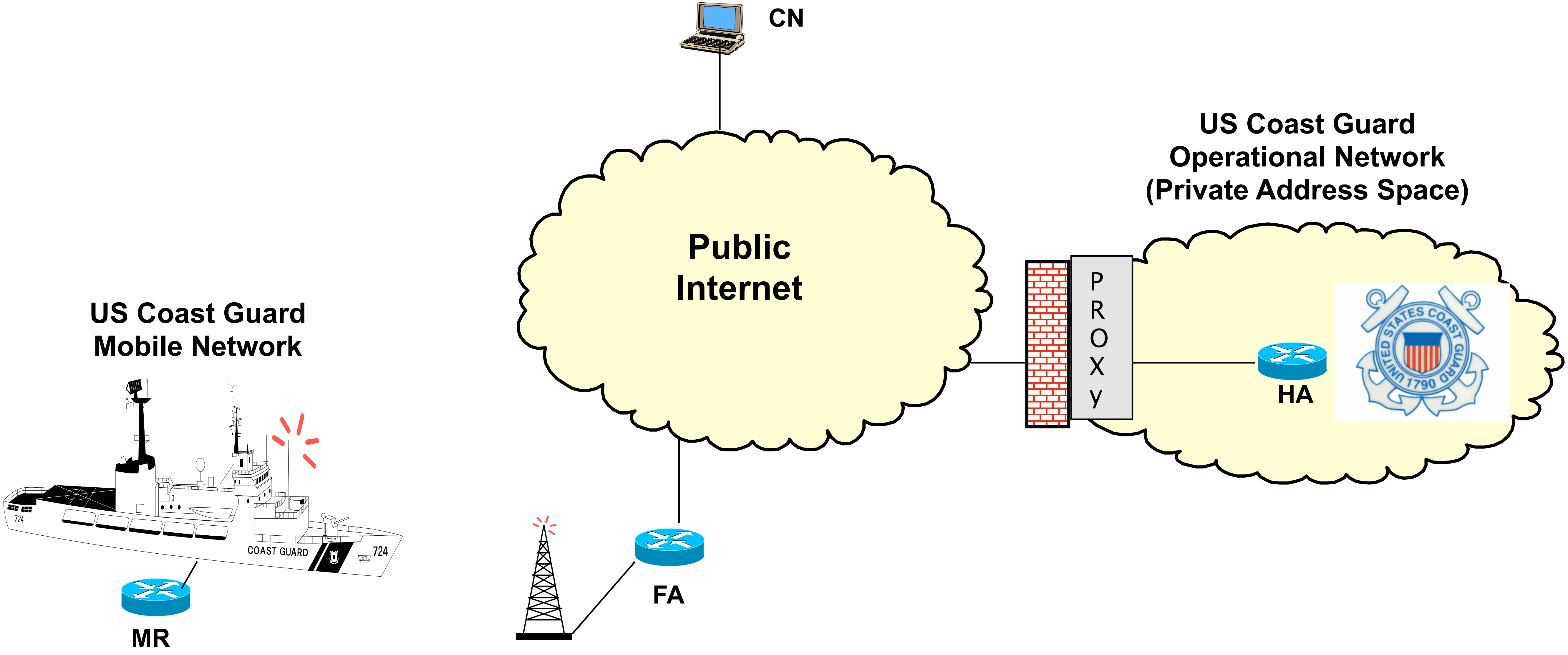
Internet

Alice (Mobile Node)

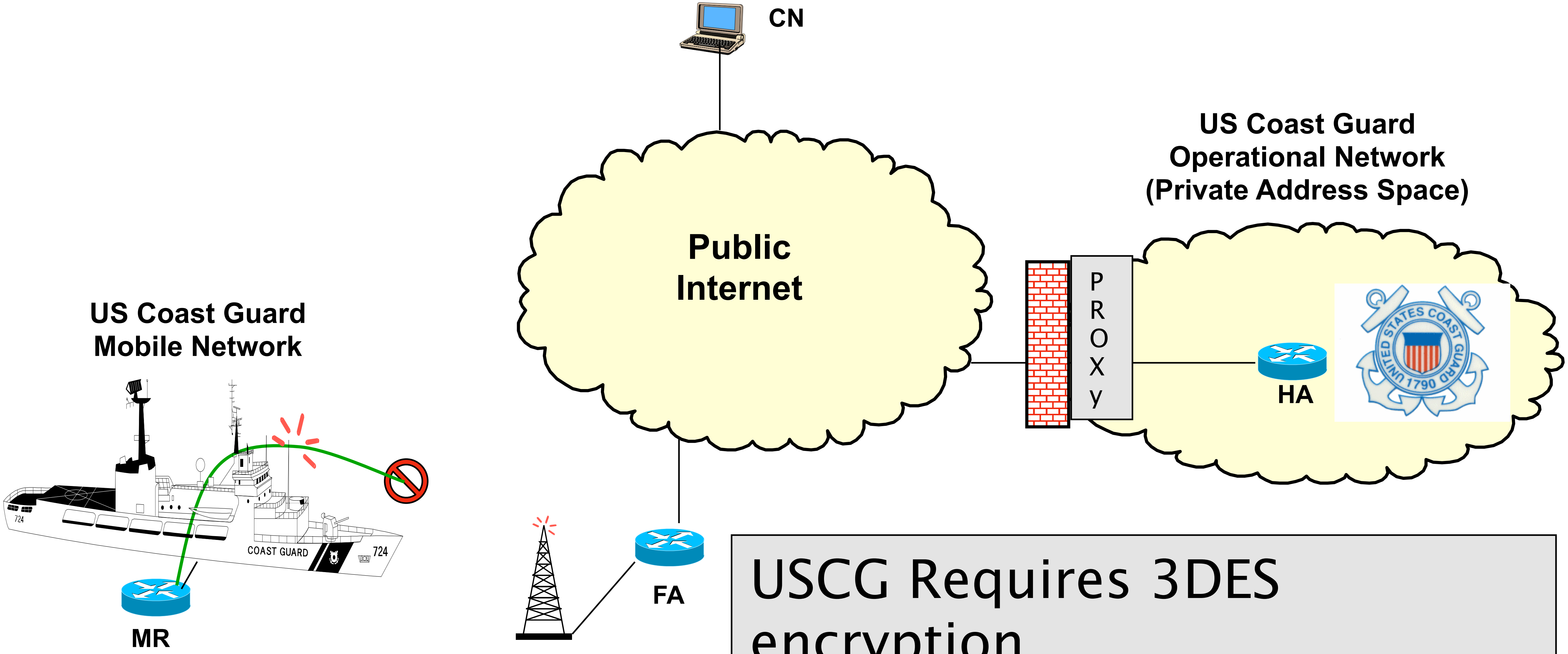
Bob (Corresponding Node)

Headquarters (Location Manager)

IPv4 "Real World" Operation

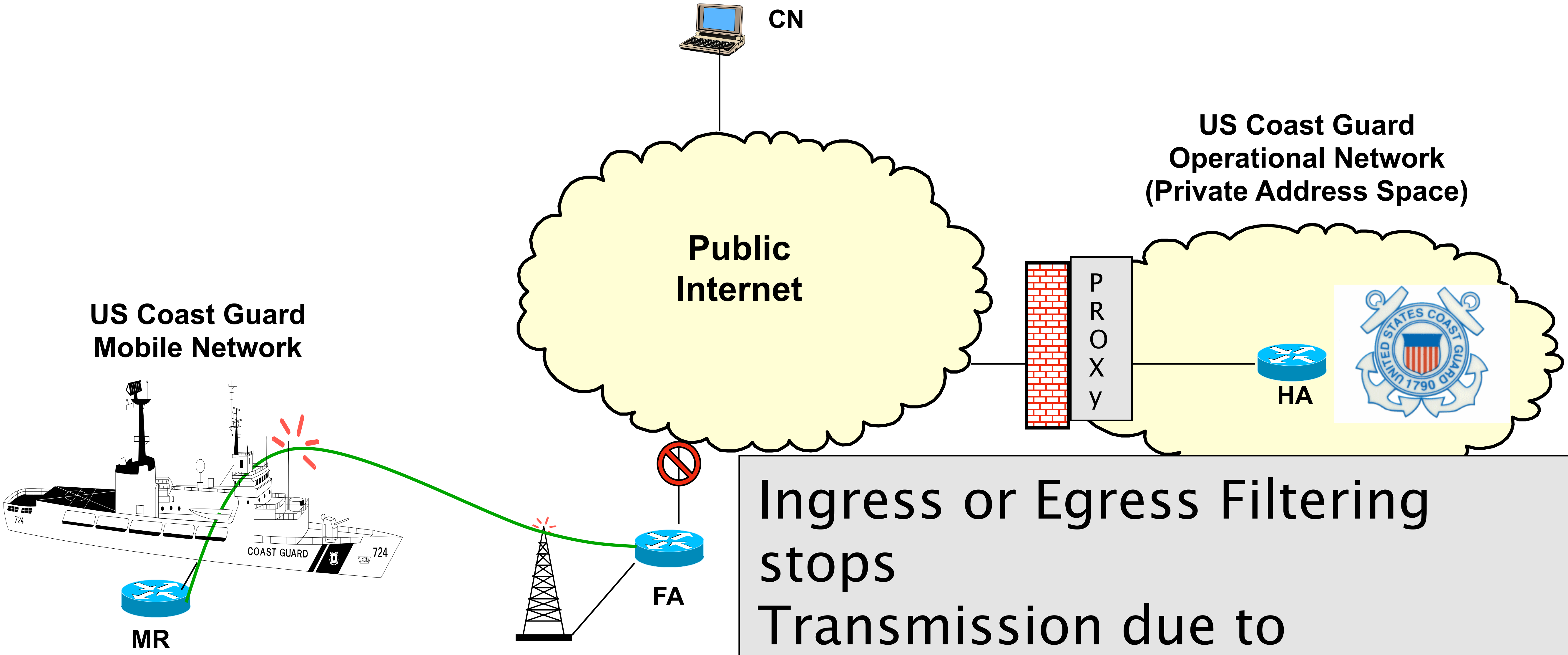

CN
Public Internet
US Coast Guard Operational Network (Private Address Space)
PROXy
HA
US Coast Guard Mobile Network
COAST GUARD
724
MR
FA

IPv4 "Real World" Operation


CN
Public Internet
US Coast Guard Operational Network (Private Address Space)
PROXy
HA
US Coast Guard Mobile Network
MR
FA
COAST GUARD
724
UNITED STATES COAST GUARD
1790

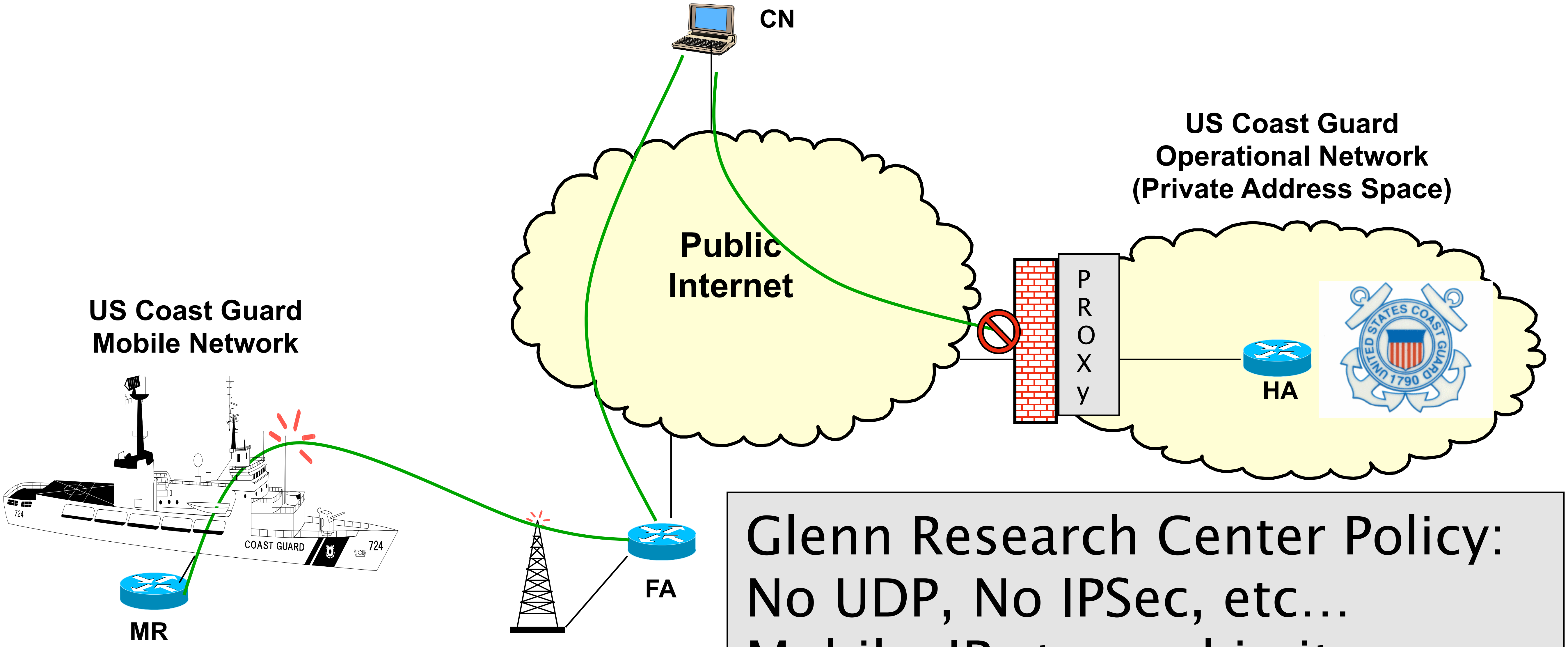
USCG Requires 3DES encryption.
WEP is not acceptable due to known deficiencies.

IPv4 "Real World" Operation



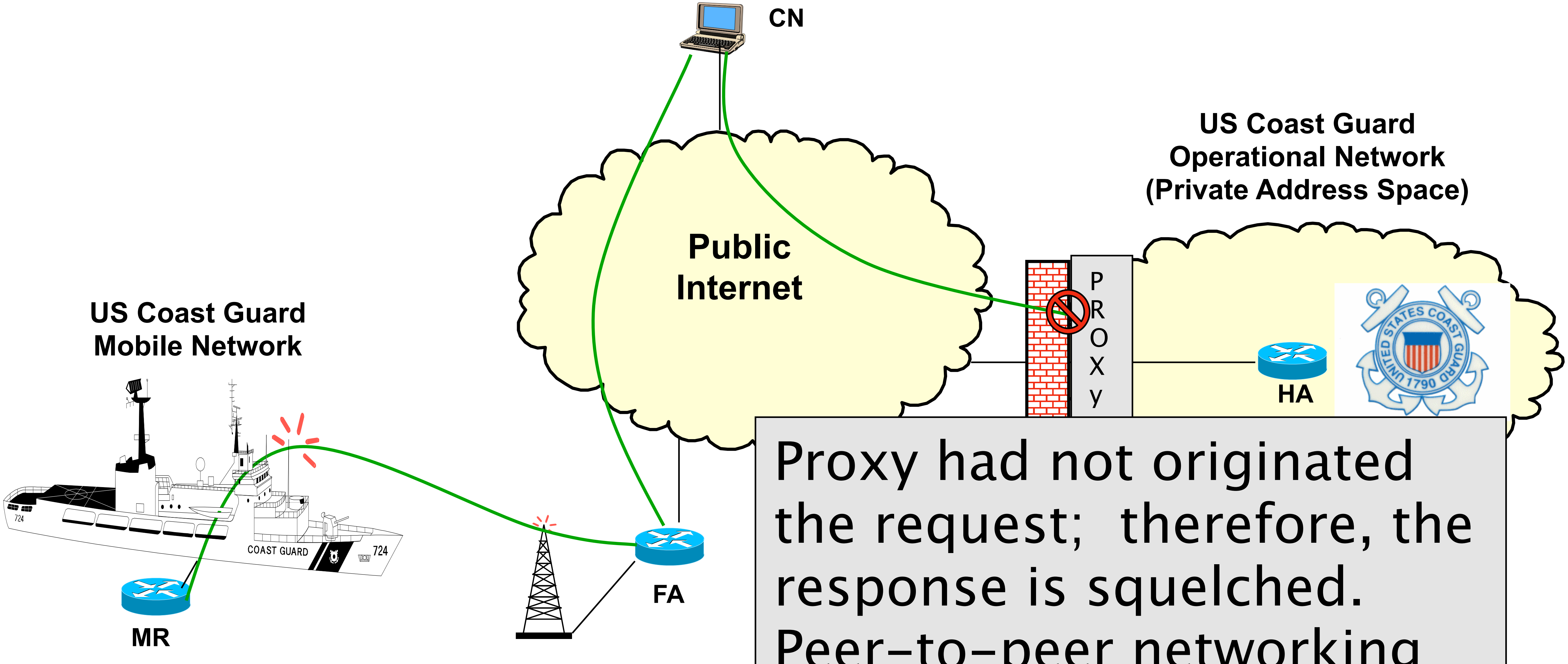
Ingress or Egress Filtering stops Transmission due to topologically Incorrect source address. IPv6 Corrects this problem.

IPv4 "Real World" Operation



Glenn Research Center Policy:
No UDP, No IPSec, etc…
Mobile-IP stopped in its tracks.
What's your policy?

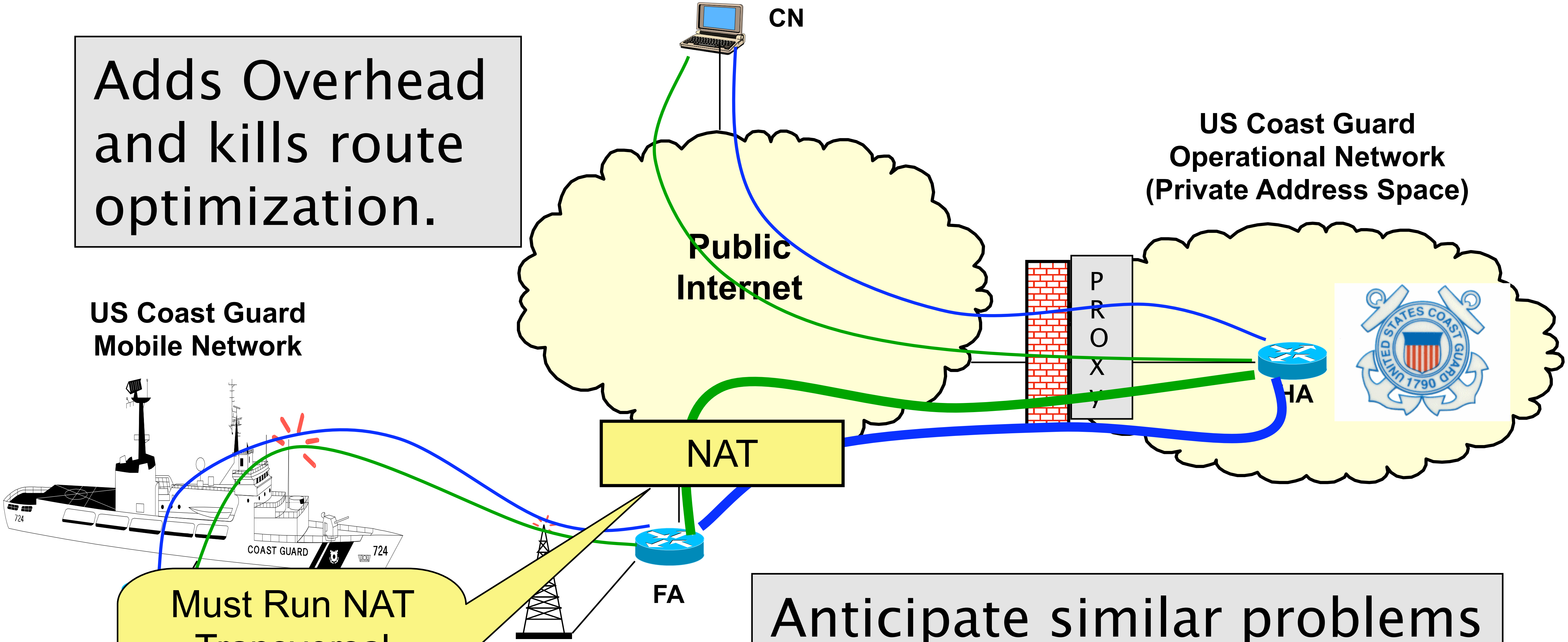
IPv4 "Real World" Operation


CN
Public Internet
US Coast Guard Operational Network (Private Address Space)
P R O X y
HA
US Coast Guard Mobile Network
COAST GUARD
724
MR
FA

Proxy had not originated the request; therefore, the response is squelched. Peer-to-peer networking becomes problematic at best.

Current Solution – Reverse Tunneling

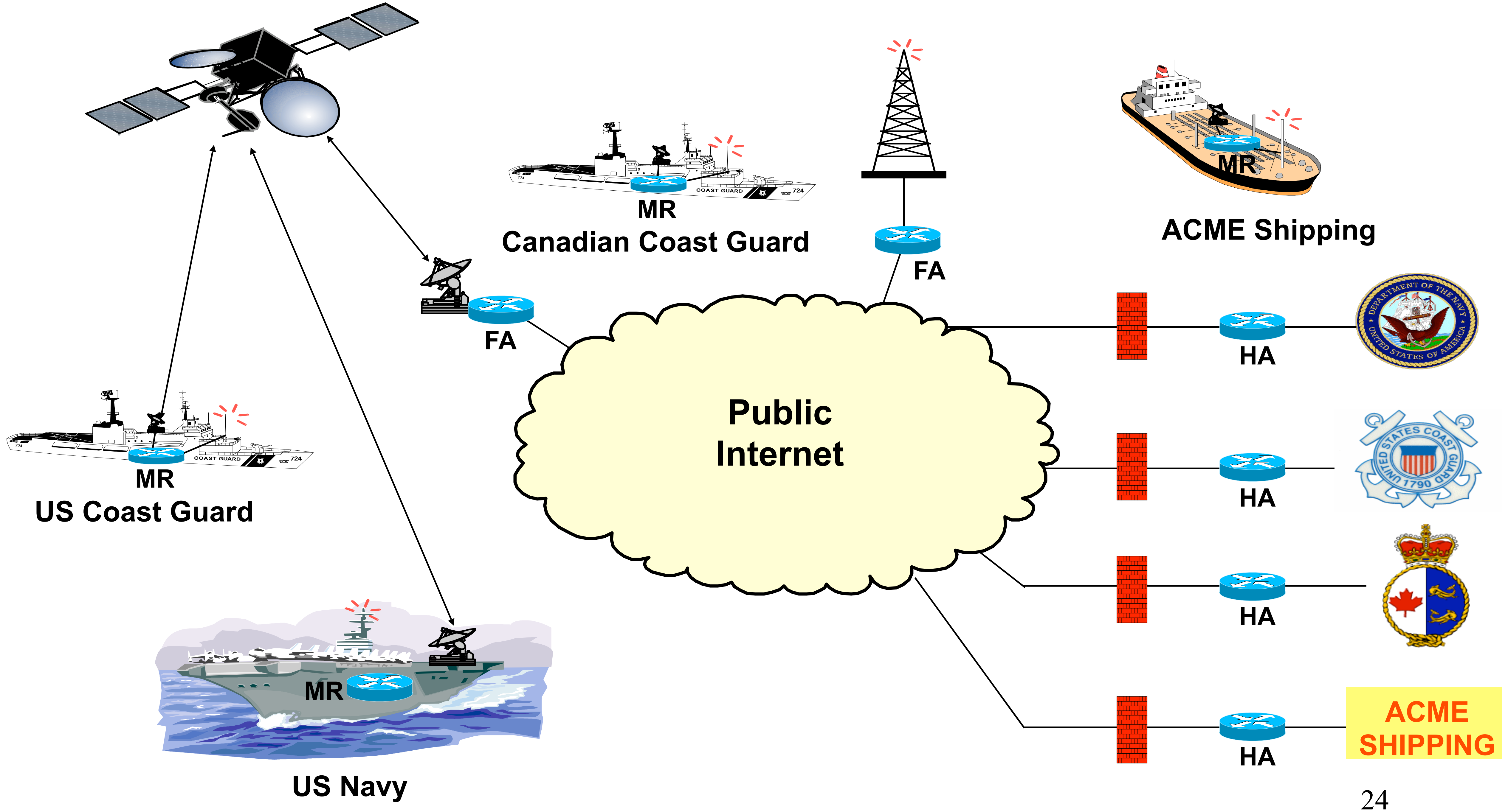
Adds Overhead and kills route optimization.


CN
US Coast Guard Operational Network (Private Address Space)
Public Internet
US Coast Guard Mobile Network
P R O X Y
HA
NAT
FA
COAST GUARD
724

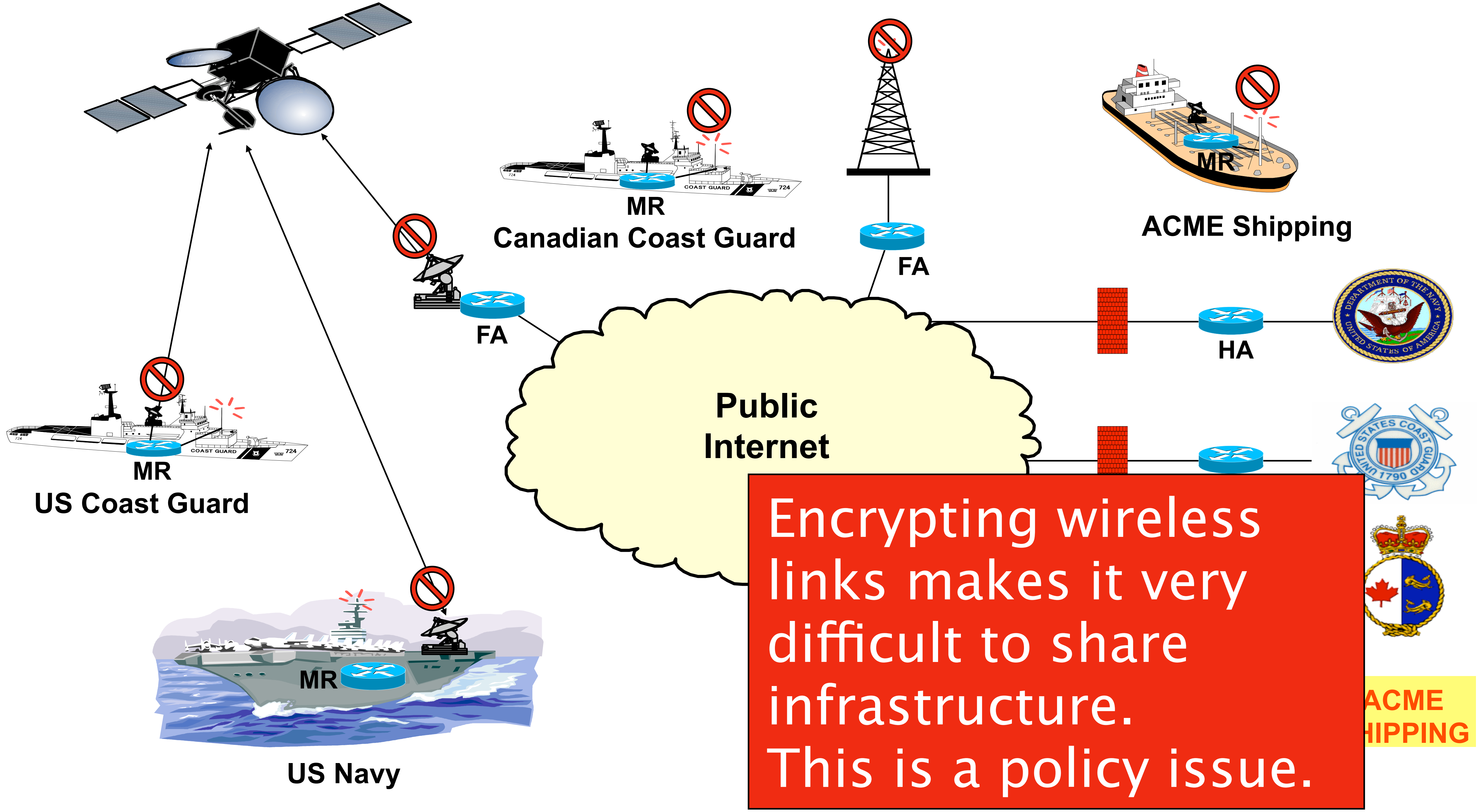
Must Run NAT Transversal Using UDP Tunnels

Anticipate similar problems for IPv6.

Shared Network Infrastructure

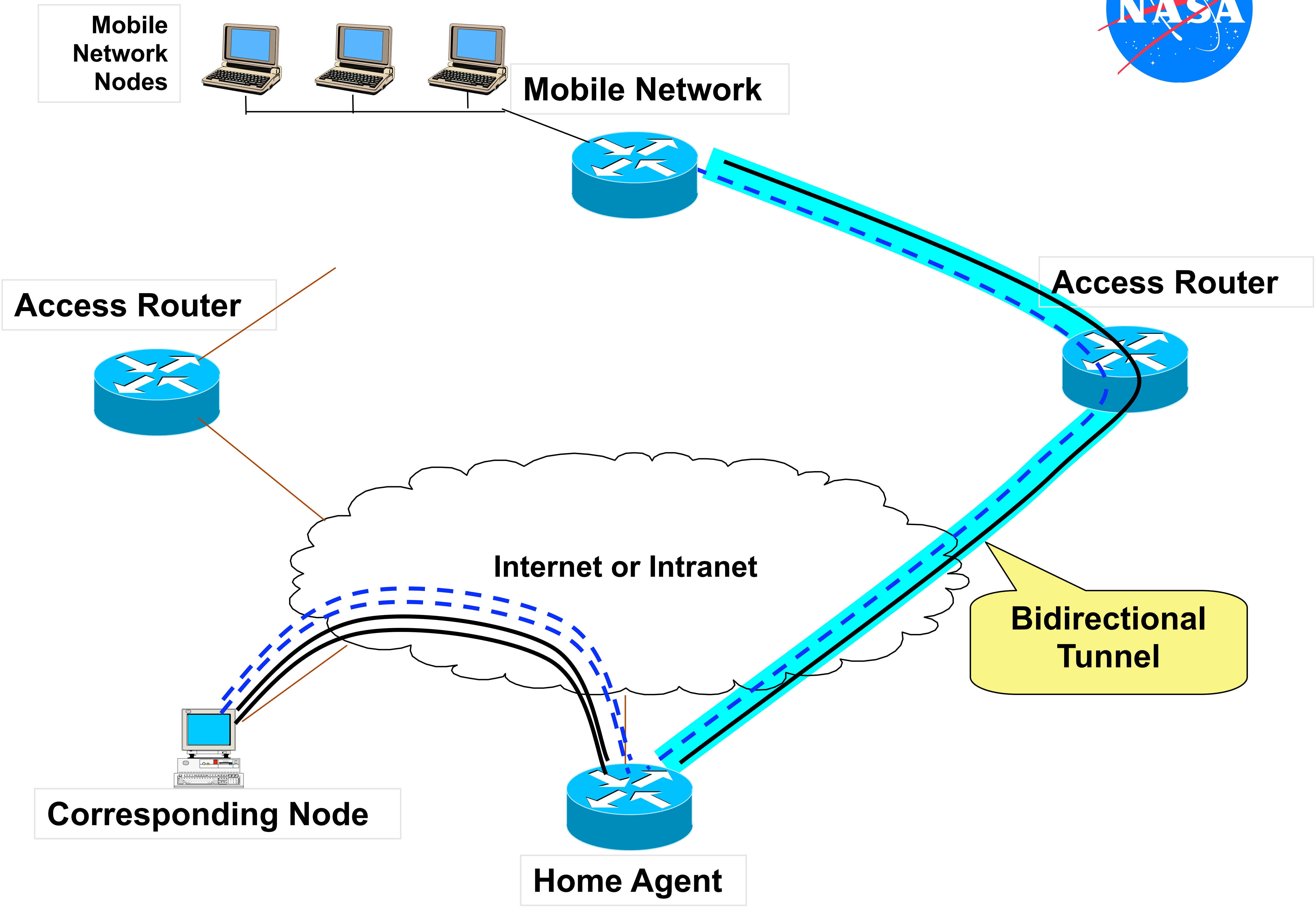


Shared Network Infrastructure

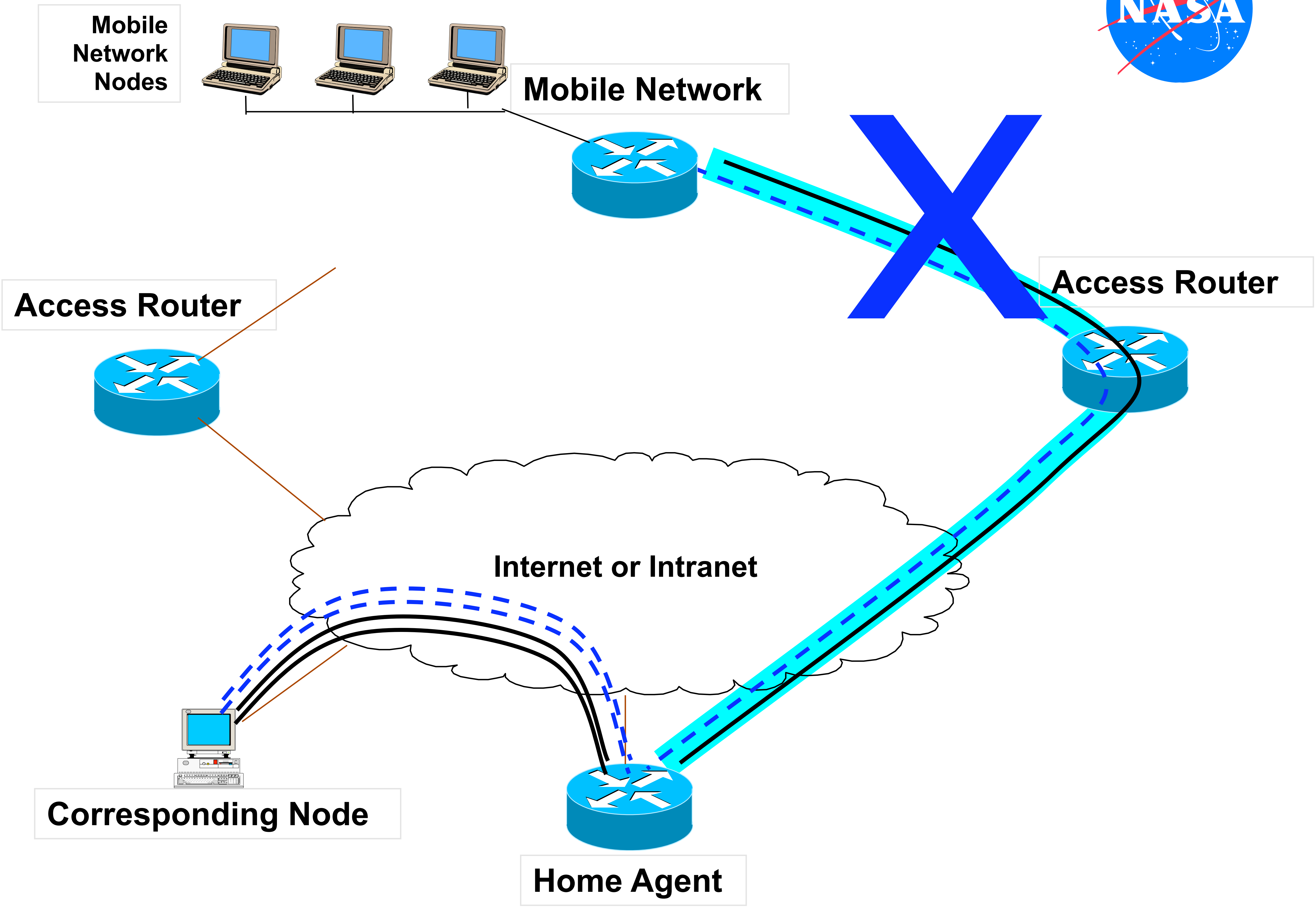


Encrypting wireless links makes it very difficult to share infrastructure.
This is a policy issue.

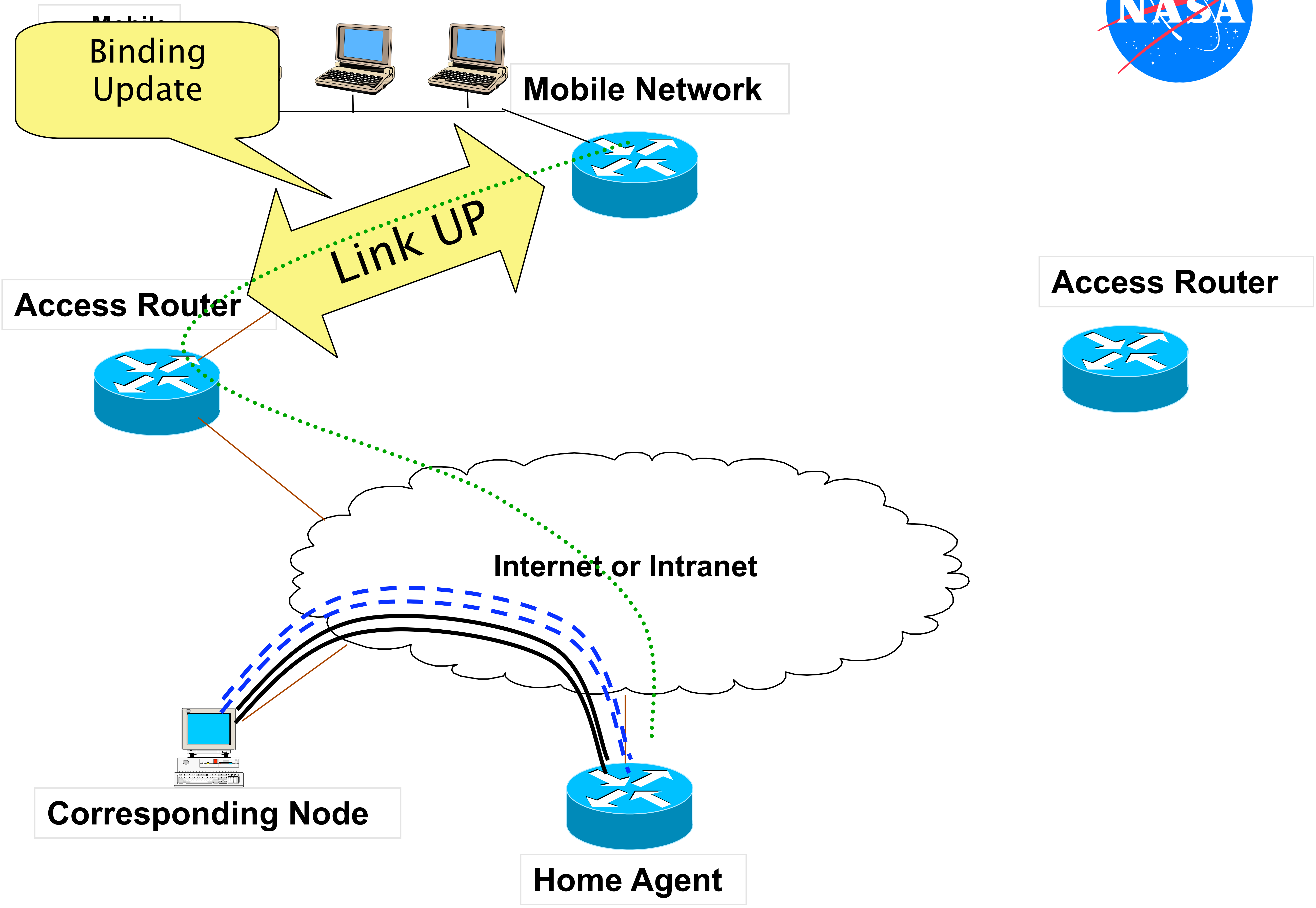
Basic Mobile Network Support for IPv6



Basic Mobile Network Support for IPv6



Basic Mobile Network Support for IPv6



Binding Update

Link UP

Mobile Network

Access Router

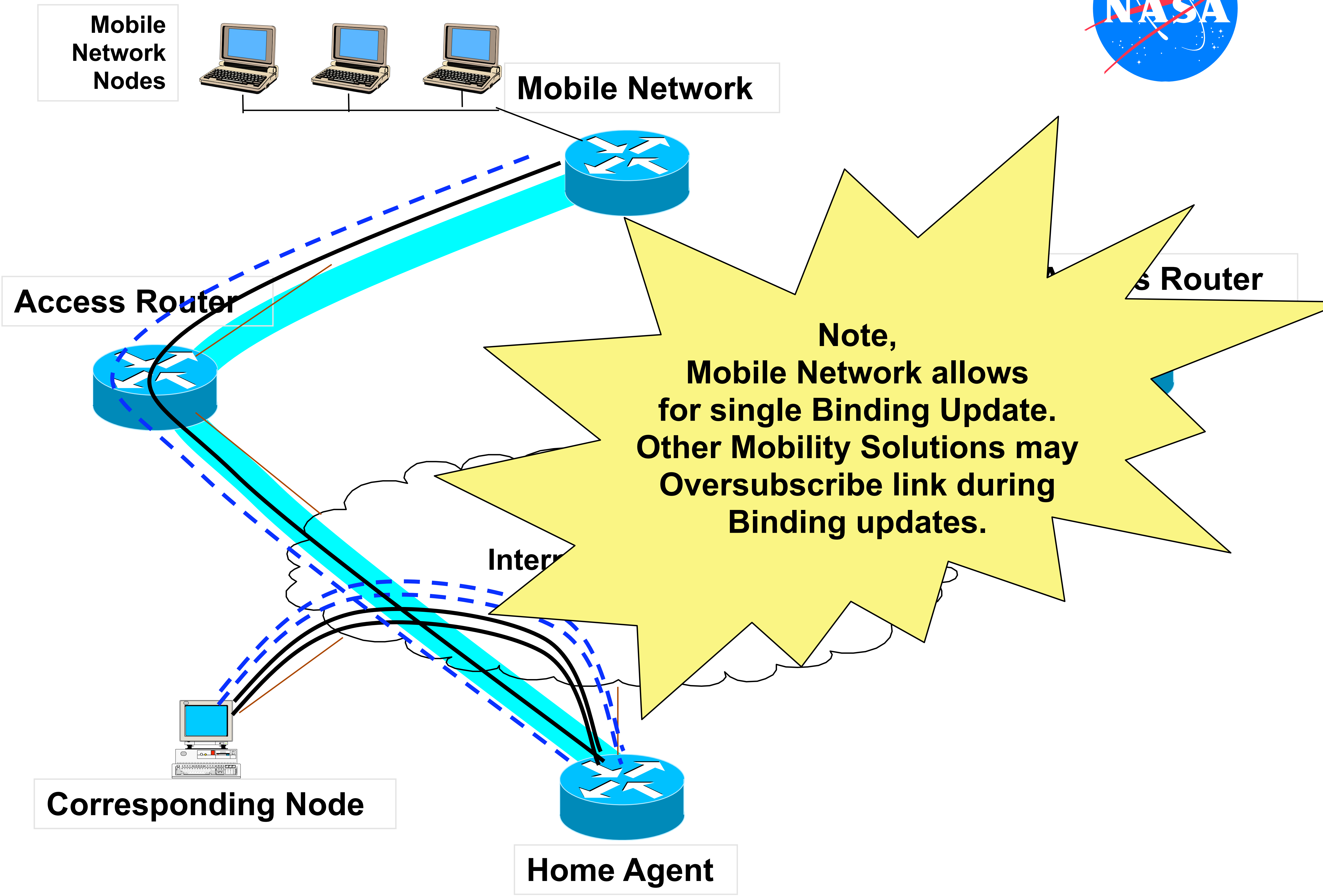
Access Router

Internet or Intranet

Corresponding Node

Home Agent

Basic Mobile Network Support for IPv6



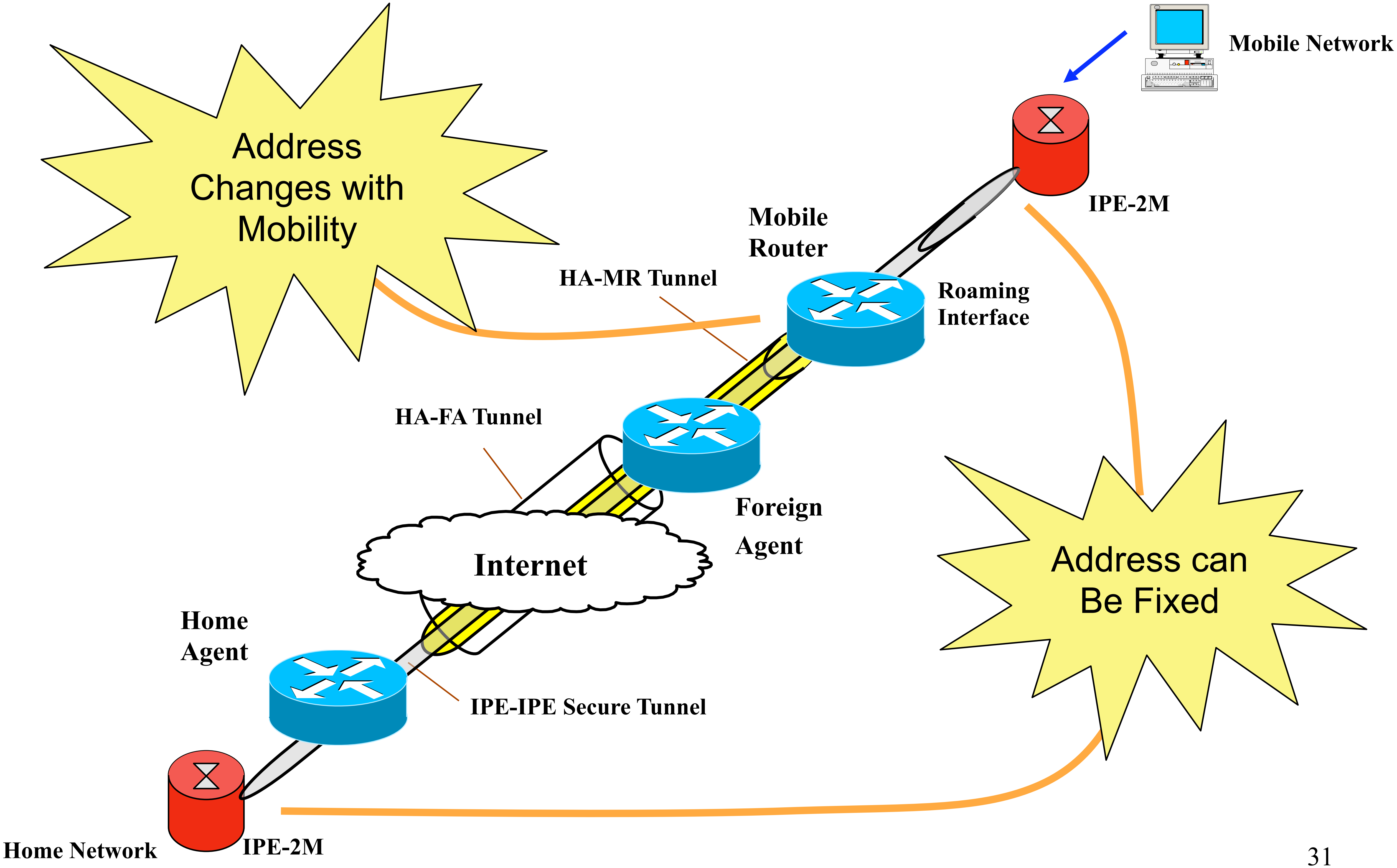
Note,
Mobile Network allows
for single Binding Update.
Other Mobility Solutions may
Oversubscribe link during
Binding updates.

Mobile Security

The Next (Current)
Research / Deployment
Area

Behind Router – Strategic

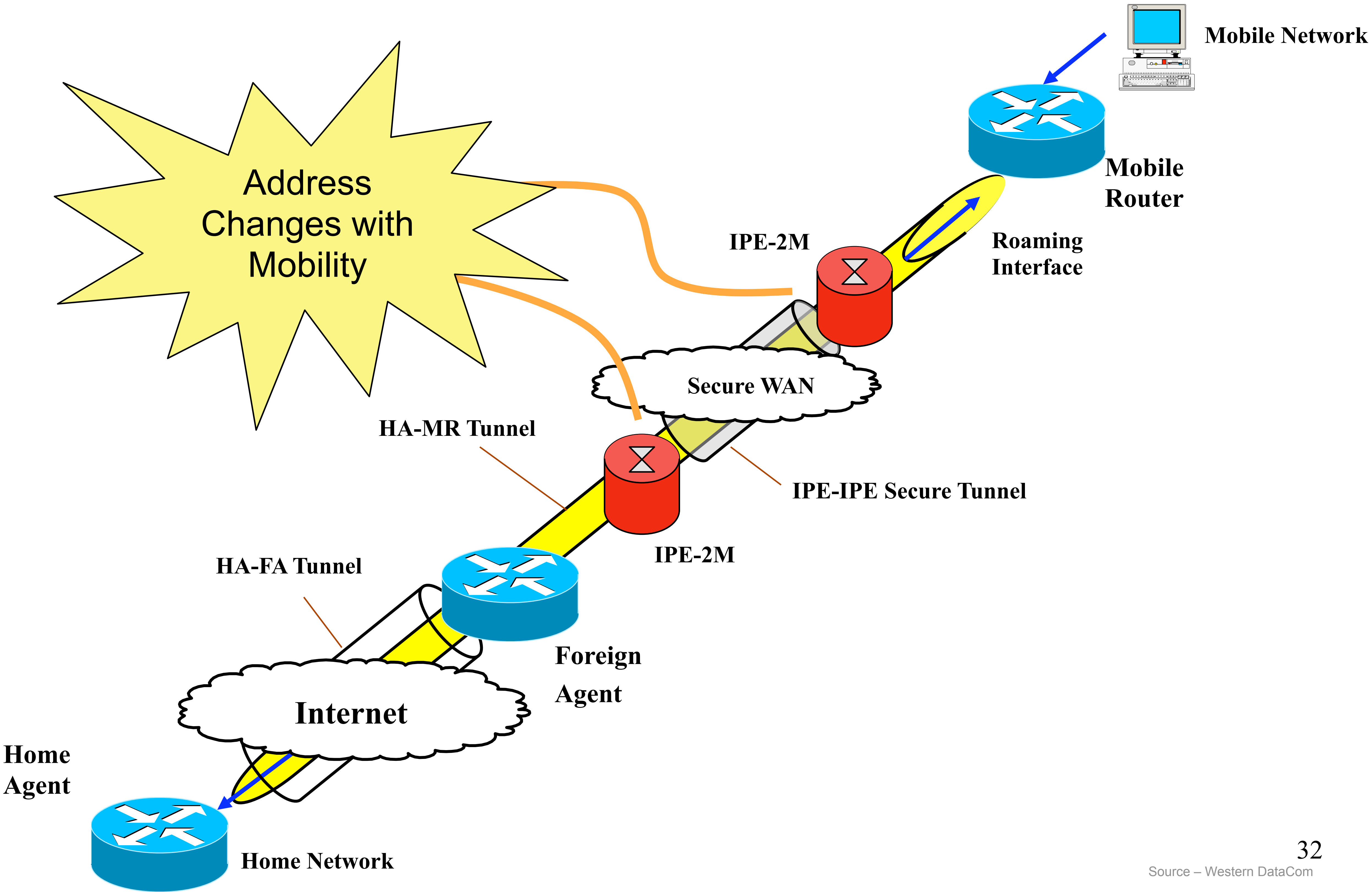
SYZYGY Engineering



Source – Western DataCom

In-Front of Router – Tactical

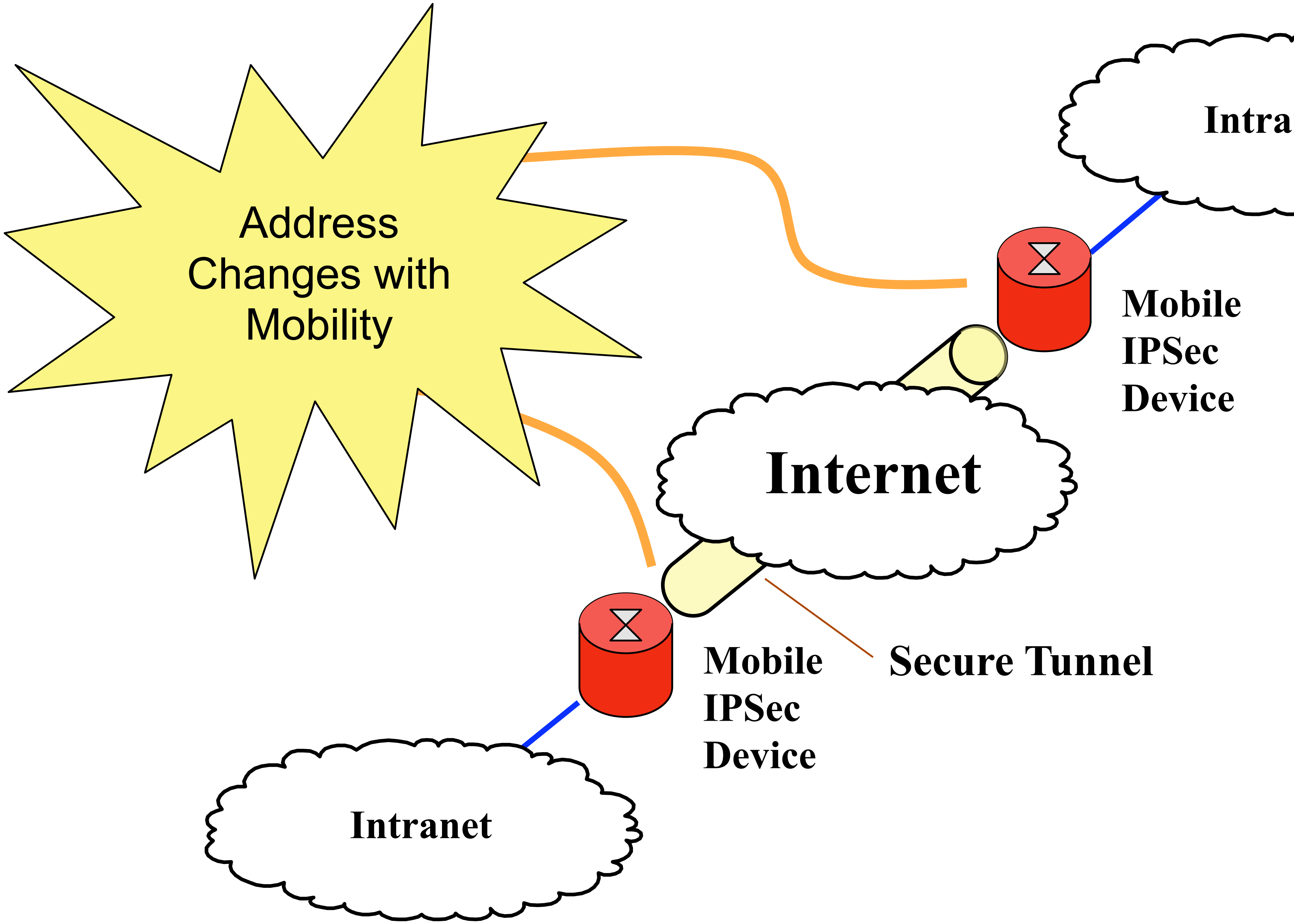
SYZYGY Engineering



Source – Western DataCom

Mobile IPSec ?

SYZYGY Engineering



Partially Being Addressed

- MOBIKE
- HIP
- Certificate Based Identity?
- Others?

IPv6 Ad Hoc Networking Challenges

SYZYGY Engineering

- **Denial of Service**
  - **Duplicate Address Detection (DAD) DoS, Uncooperative Router, etc…**
  - **Neighbor Discovery trust and threats**
- **Network Discovery**
  - **Reachback, DNS, Key Manager**
- **Security**
  - **IPSec / HAIPES tunnel end-points**
  - **Security Policies in a dynamic environment**
  - **Is layer-2 encryption sufficient security?**
  - **Insecure routing**
    - **Attackers may inject erroneous routing information to divert network traffic, or make routing inefficient**
- **Key Management**
  - **Lack of key distribution mechanism**
  - **Hard to guarantee access to any particular node (e.g. obtain a secret key)**

IPv6 Ad Hoc Networking Challenges

- **Duplicate Address Discovery**
  - Not suitable for multi-hop ad hoc networks that have dynamic network topology
  - Need to address situation where two MANET partitions merge
- **Radio Technology**
  - Layer-2 media access often incompatible with layer-3 MANET routing protocol
- **Battery exhaustion threat**
  - A malicious node may interact with a mobile node very often trying to drain the mobile node’s battery
- **Testing of Applications**
- **Integrating MANET into the Internet**

Host Identity Protocol
as an IP-layer mobility solution

INFOCOM Mobility panel
Thursday, March 17 2005

Pekka Nikander
Ericsson Research Nomadiclab and
Helsinki Institute for Information Technology
http://www.hip4inter.net

Presentation outline

- A brief history of HIP
- HIP in a Nutshell
- HIP and IP-layer mobility

A Brief History of HIP

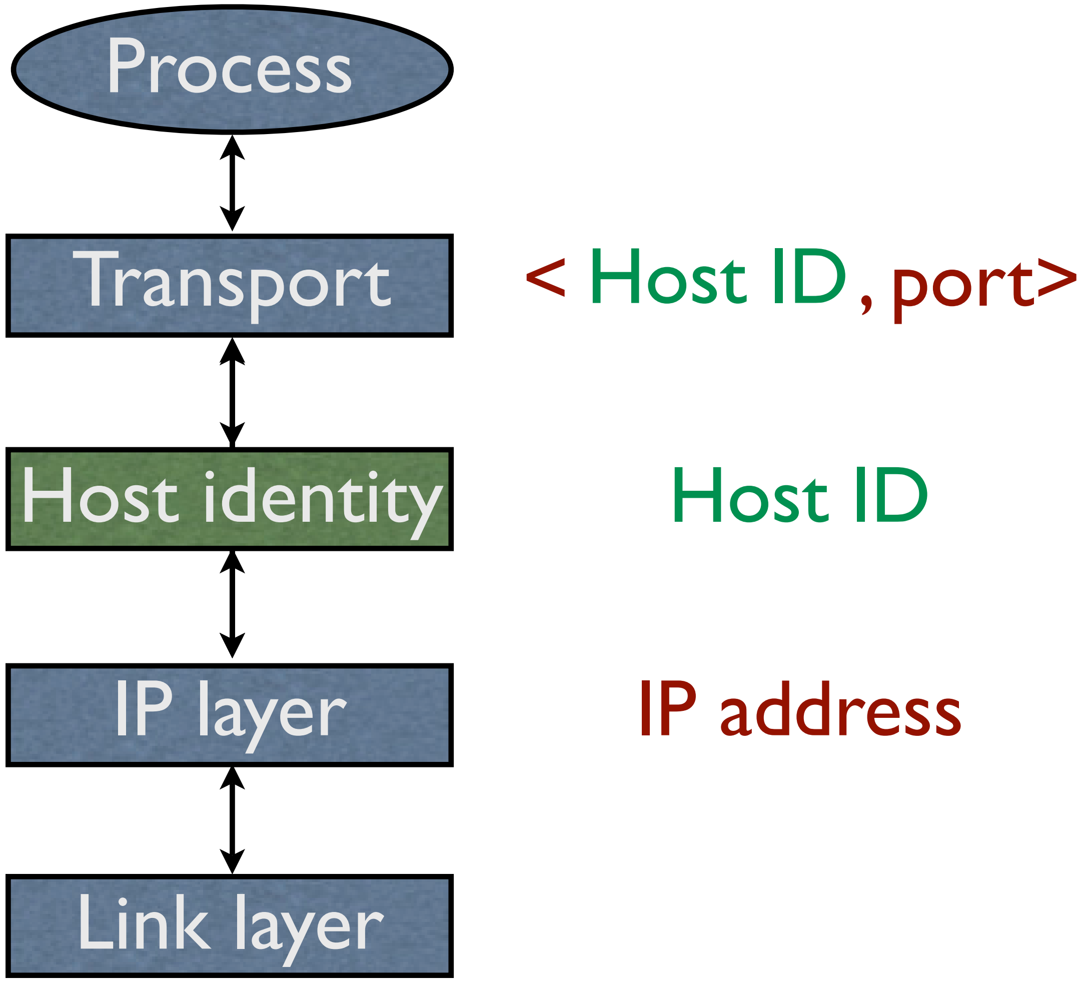
- Idea discussed briefly at 47th IETF in 1999
- Development "aside" the IETF
- IETF WG and IRTF RG created in early 2004
- Base protocol more or less ready
  - Four interoperating implementations
- More work needed on advanced mobility, multi-homing, NAT traversal, infrastructure, and other issues

HIP in a Nutshell

- Architectural change to TCP/IP structure
- Integrates security, mobility, and multi-homing
  - Opportunistic host-to-host security (ESP)
  - End-host mobility, across IPv4 and IPv6
  - End-host multi-homing, across IPv4 / v6
  - IPv4 / v6 interoperability for apps
- A new layer between IP and transport
  - Introduces cryptographic Host Identifiers

The Idea

- A new Name Space of Host Identifiers (HI)
    - Public crypto keys!
    - Presented as 128-bit long hash values, Host ID Tags (HIT)
- Sockets bound to HIs, not to IP addresses
- HIs translated to IP addresses in the kernel



Process

Transport

Host identity

IP layer

Link layer

< Host ID, port>

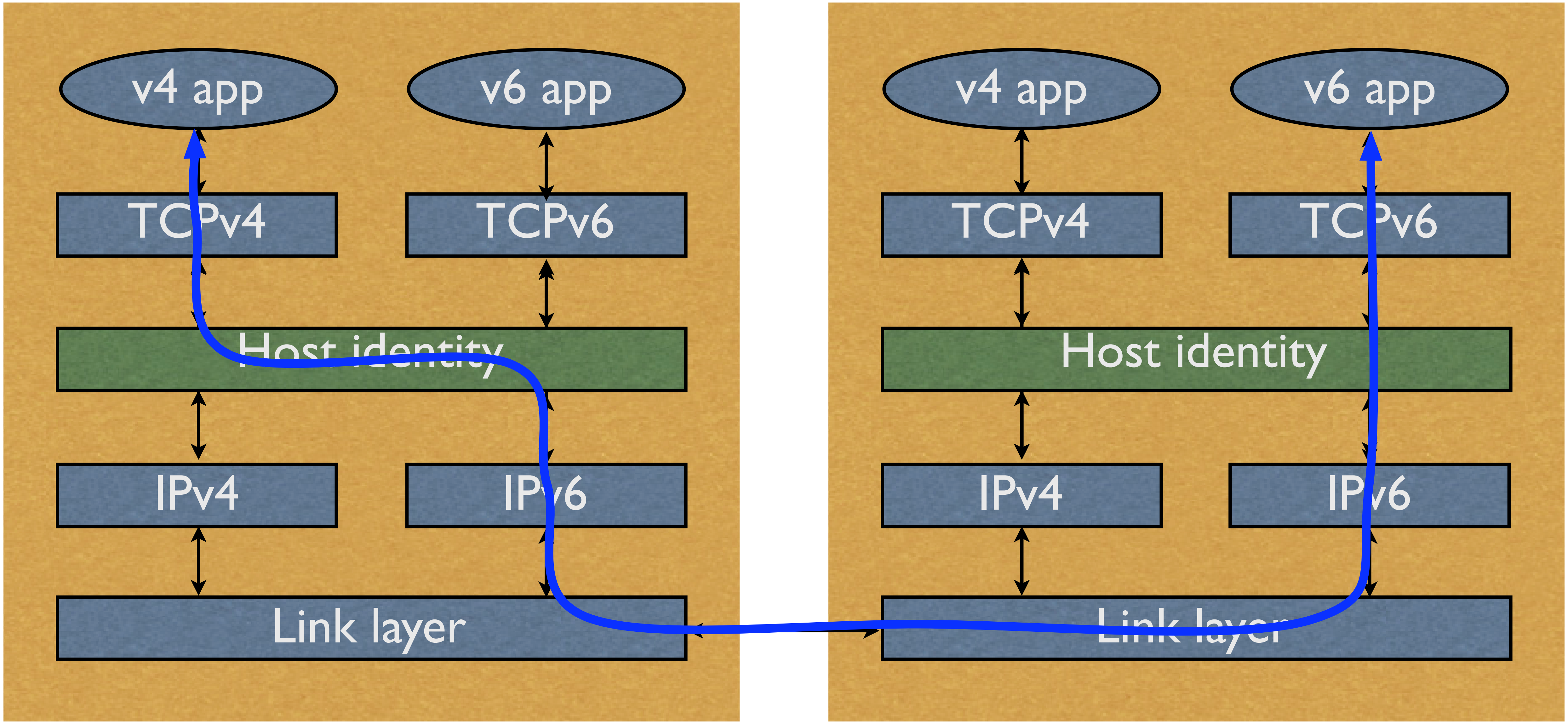
Host ID

IP address

Many faces of HIP

- More established views:
  - A different IKE for simplified end-to-end ESP
  - “Super” Mobile IP with v4/v6 interoperability and dynamic home agents
  - A host-based multi-homing solution
- Newer views:
  - New waist of IP stack; universal connectivity
  - Secure carrier for signalling protocols

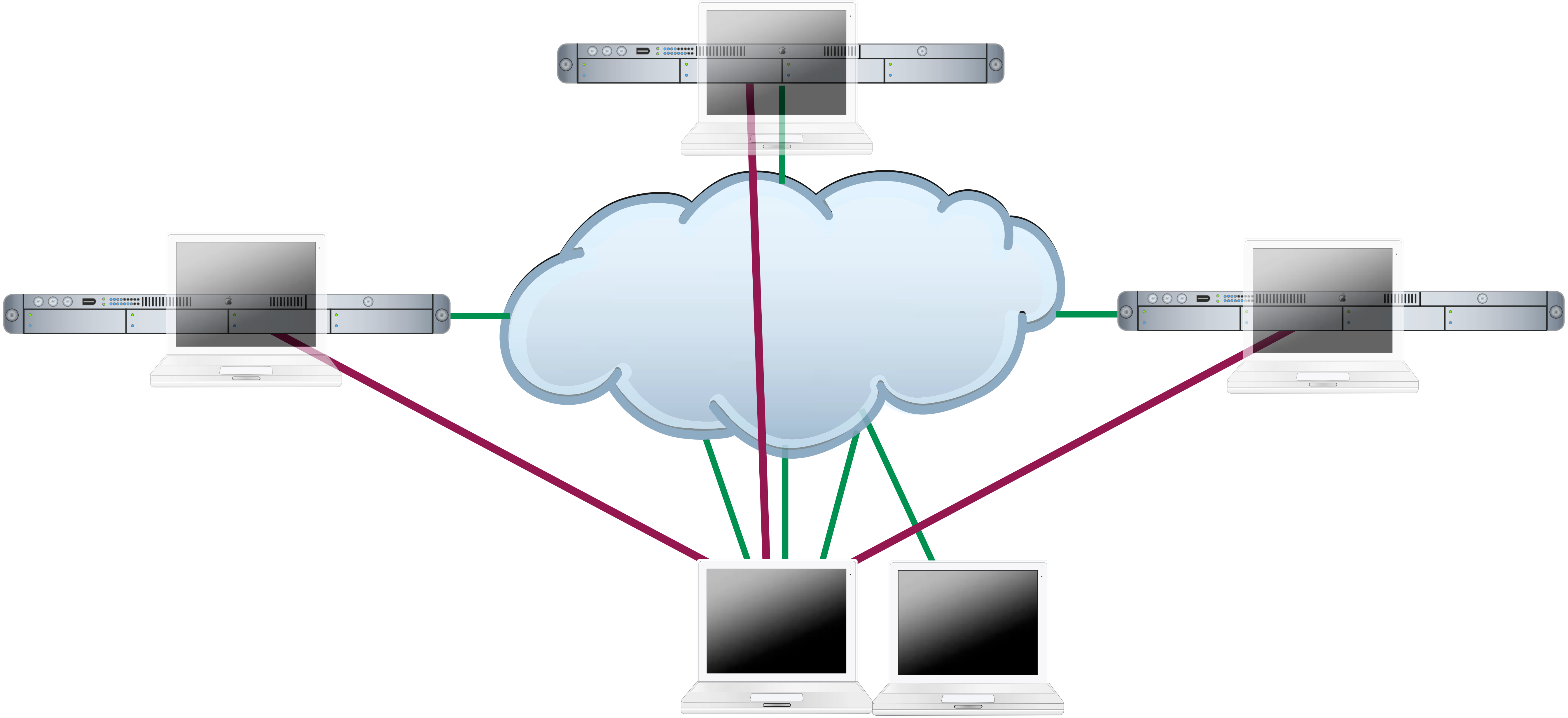
HIP as the new waist of TCP/IP



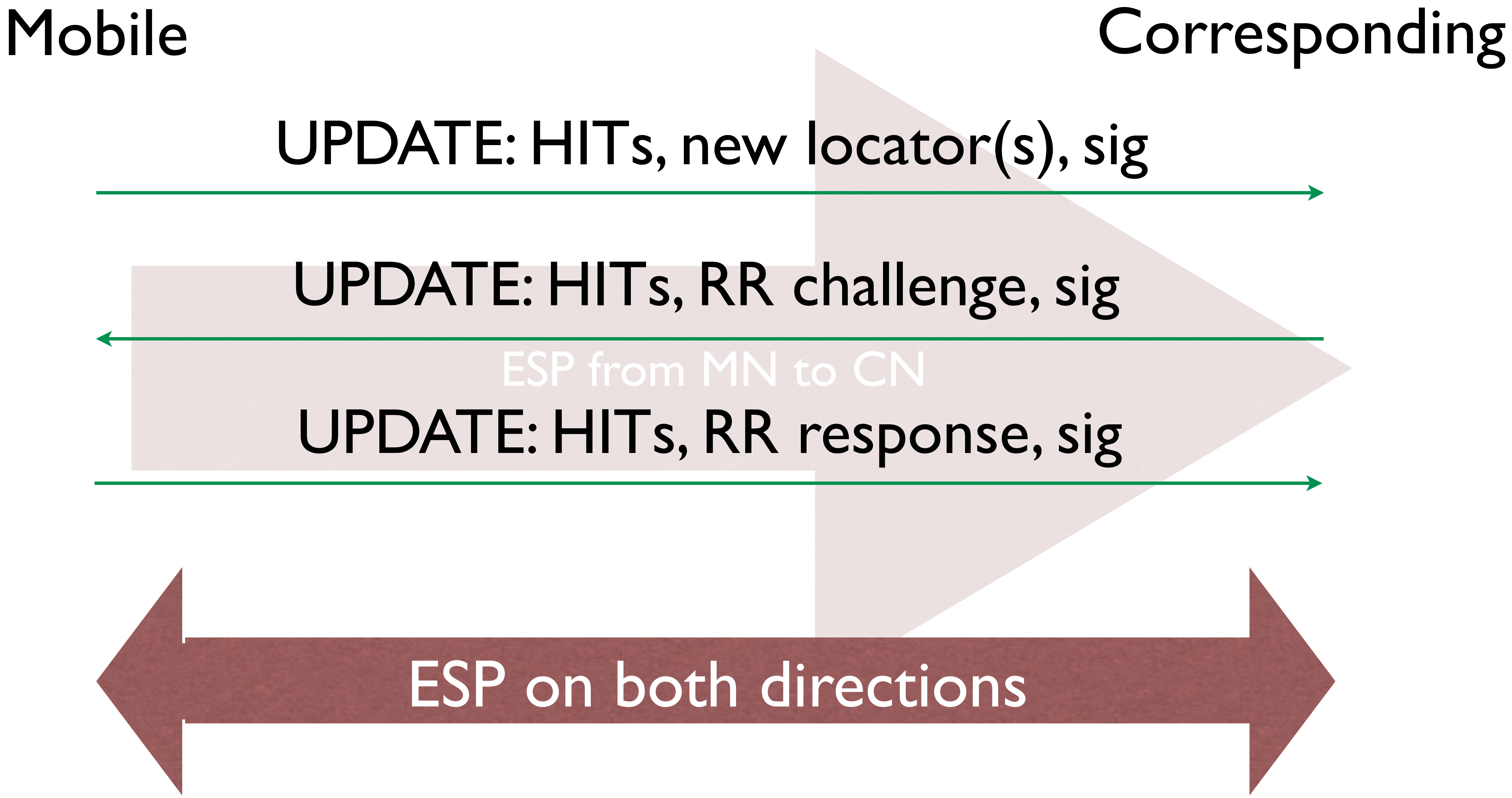
HIP Mobility

- In HIP mobility and multi-homing become duals of each other
  - Mobile host has many addresses over time
  - Multi-homed host has many addresses at the same time
- Leads to a “Virtual Interface” Model
  - A host may have real and virtual interfaces
  - Subsumes the “Home Agent” concept

Virtual Interface Model



HIP Mobility protocol



Mobile

Corresponding

UPDATE: HITs, new locator(s), sig

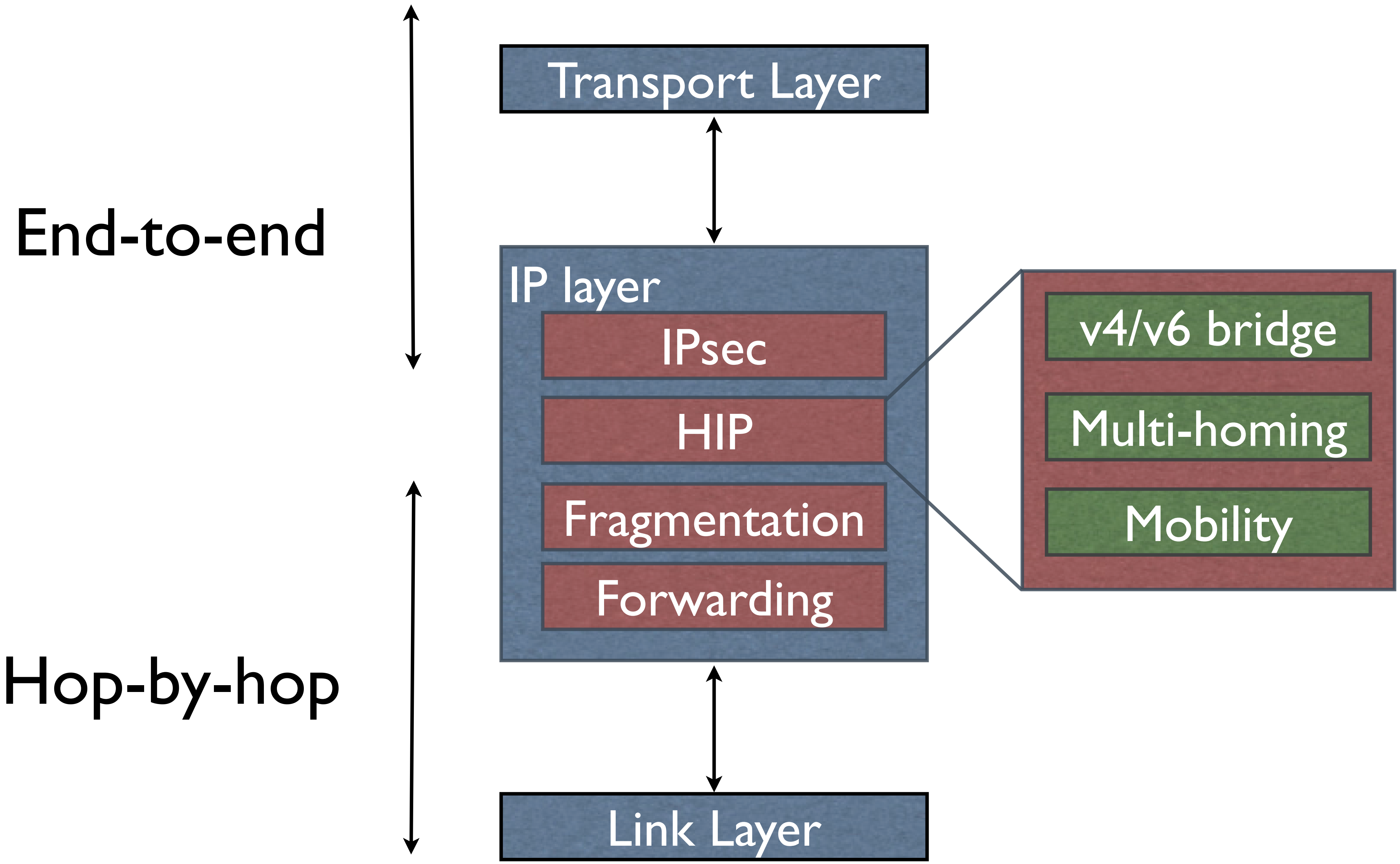
UPDATE: HITs, RR challenge, sig

ESP from MN to CN

UPDATE: HITs, RR response, sig

ESP on both directions

More detailed layering



Benefits of HIP mobility

- Mobility combined with multi-homing
- Mobility over both IPv4 and IPv6
- Built-in baseline security and route optimisation
- No single point of failure
  - Possibility to change forwarding agents dynamically
- Relatively simple implementation (12000 LoC)

Future of HIP-based mobility

- Streamline signalling with recent ideas
  - From 1.5 RTT to 0.5 RTT e2e delay
- Combine cryptographic delegation w/ mobility:
  - MNs can delegate mobility signalling to a mobile router in a moving network (NEMO)
  - Application mobility (process migration) becomes more approachable
- Support NAT traversal

Fitting Mobility Into the Internet Layer Scheme

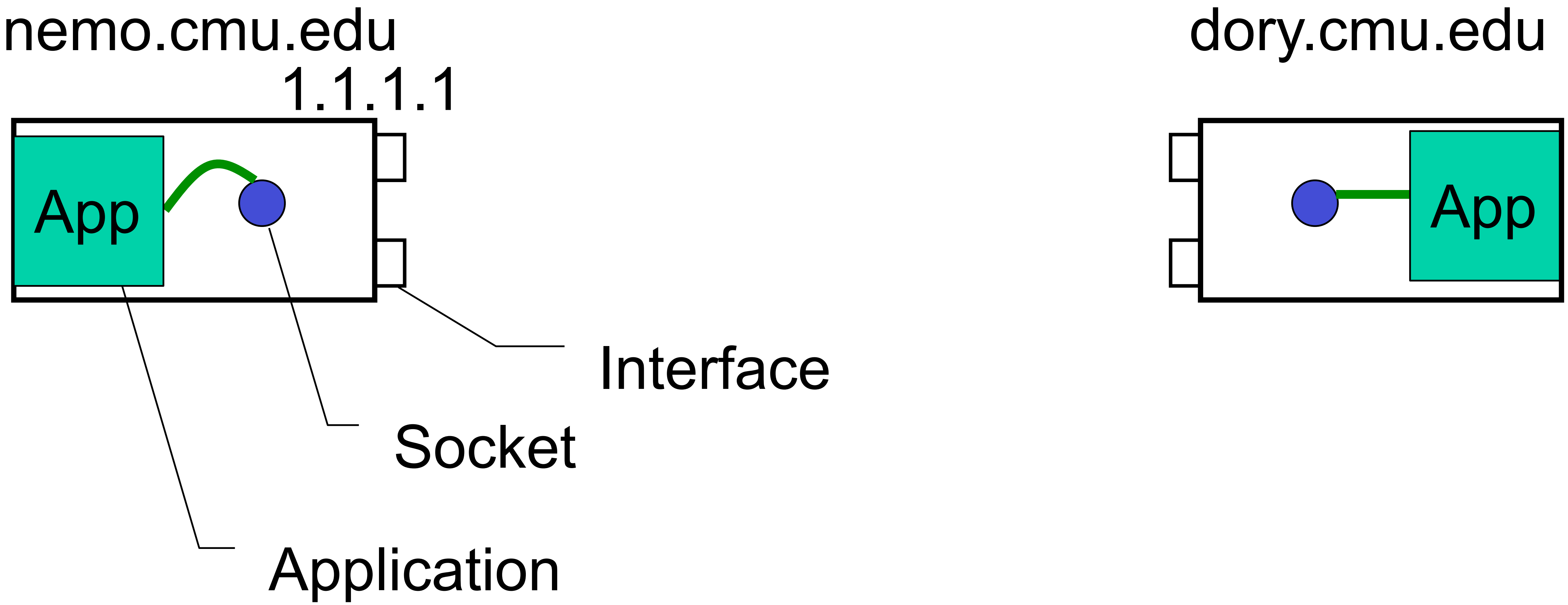
Session/Transport Layer Mobility

David A. Maltz

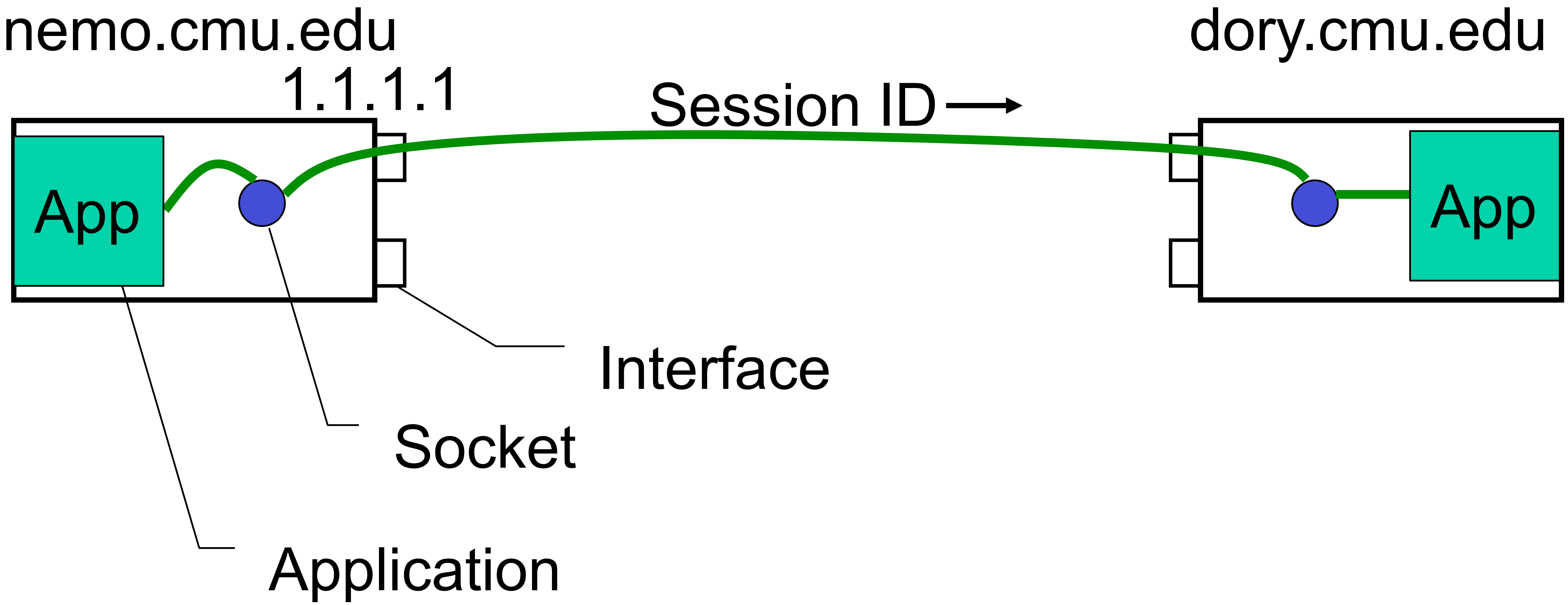
Carnegie Mellon University

dmaltz@cs.cmu.edu

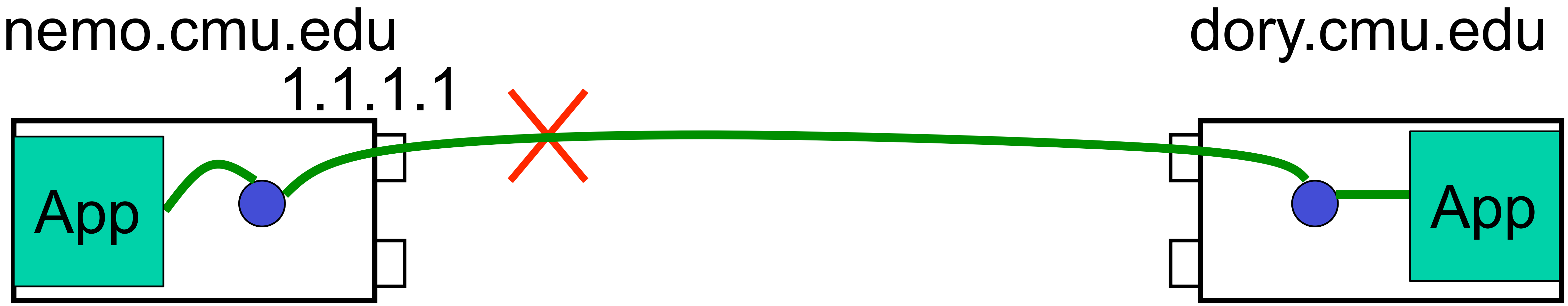
Session Layer Mobility



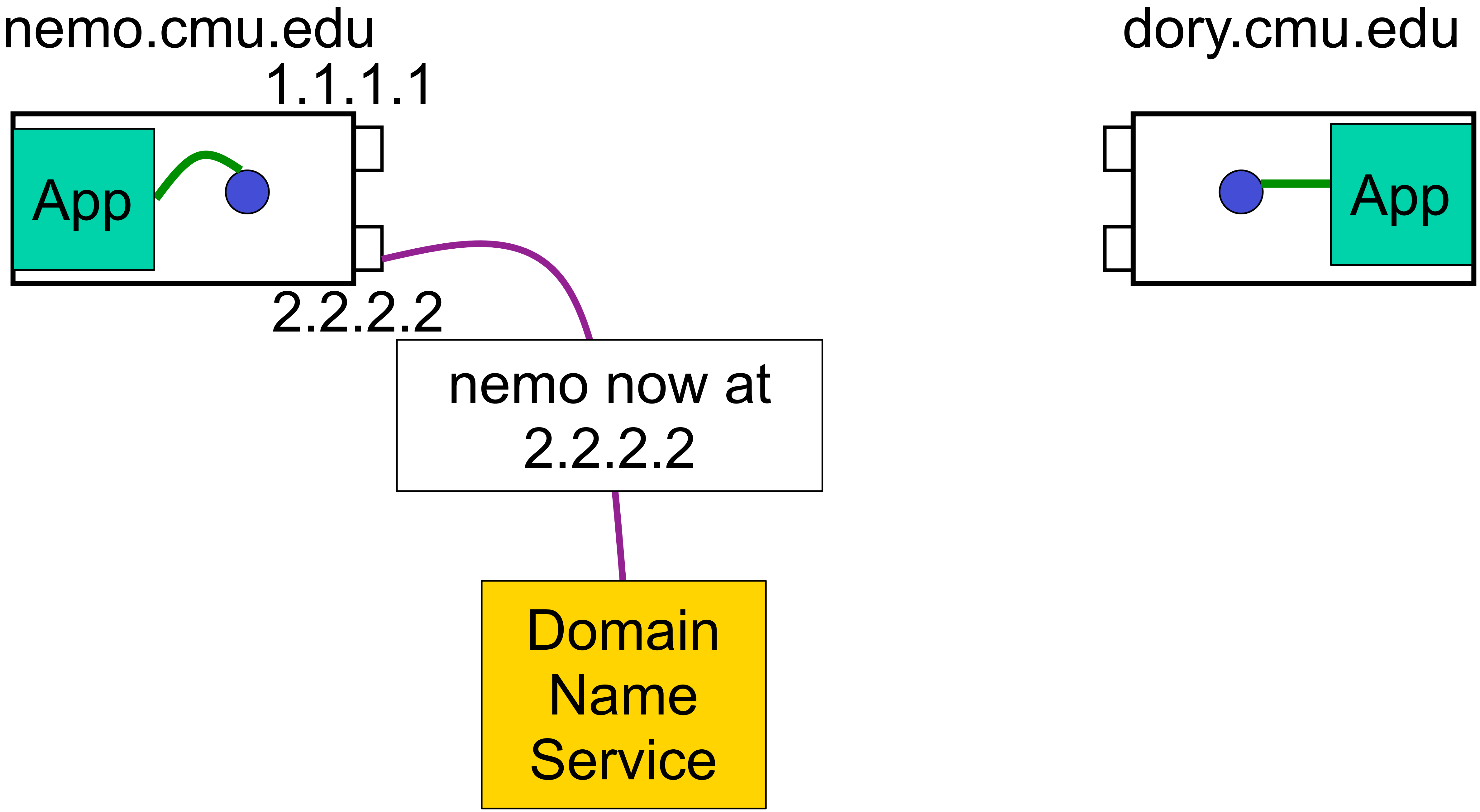
Session Layer Mobility



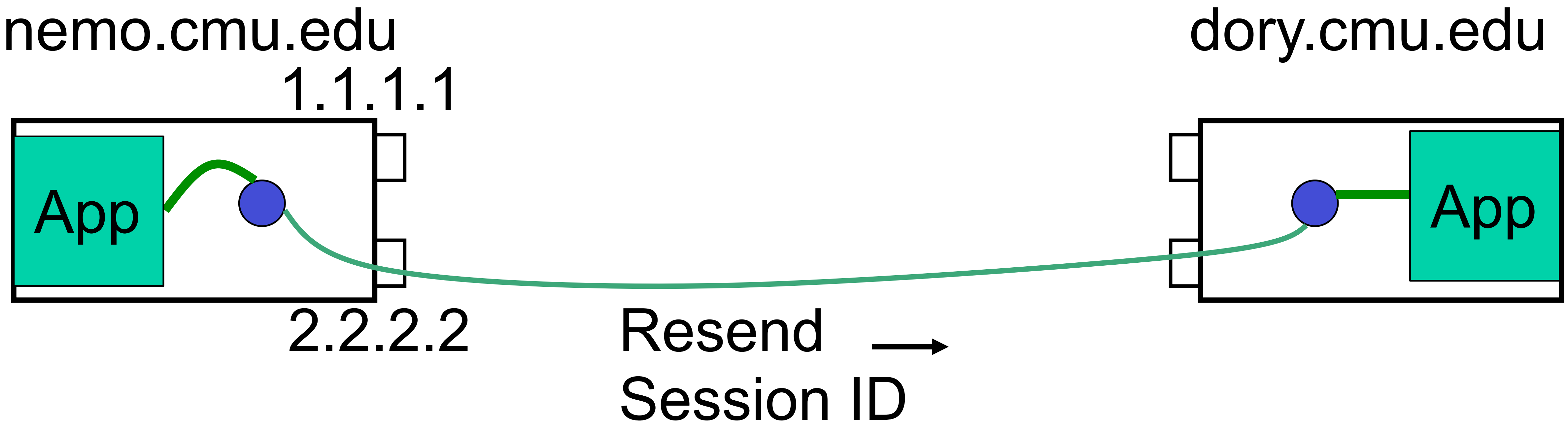
Session Layer Mobility



Session Layer Mobility



Session Layer Mobility



Pros/Cons of Session Layer Control

Pro: Can avoid triangle routing

Pro: Interfaces use topologically correct address

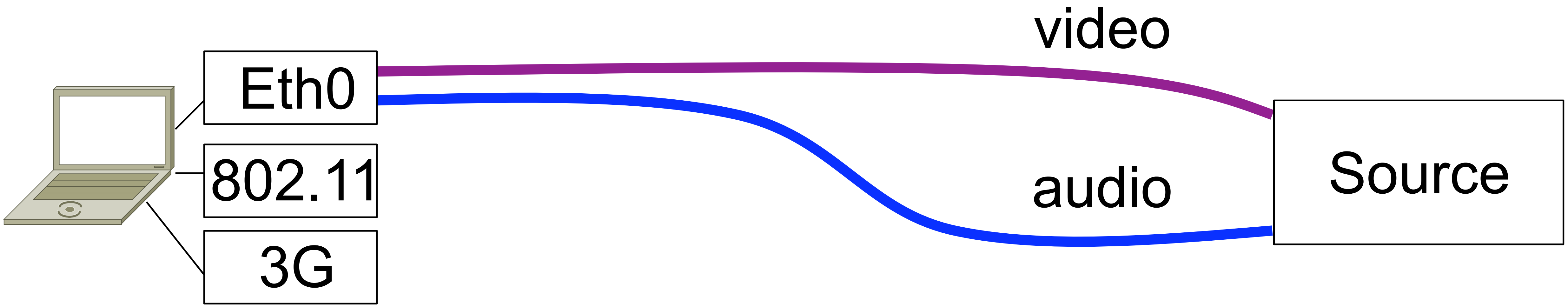
- Fewer problems with ingress/egress filters

Con: Need help changing addresses

- External support required for:
  - Detecting when host has moved
  - Obtaining new address
- Mobile IPv4 provides Agent Advertisements

Pros/Cons of Session Layer Control

Pro: Per-session control over mobility

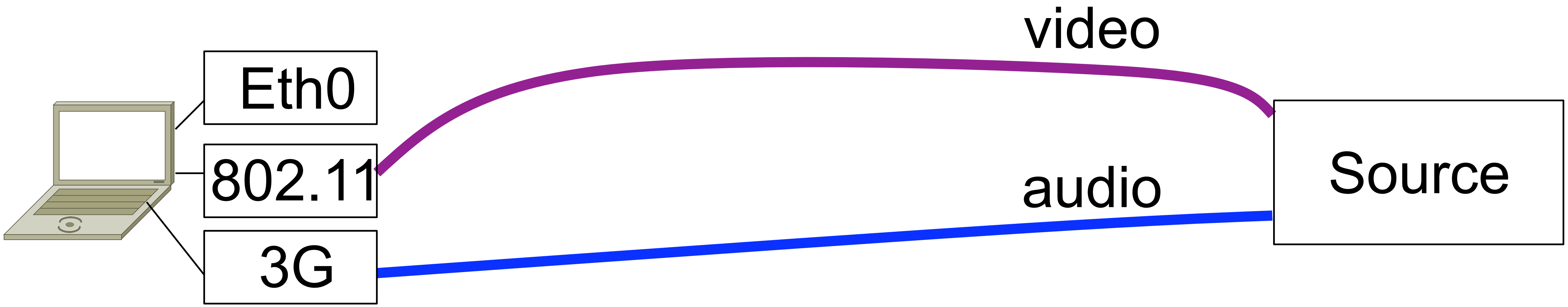


A laptop user attends a video conference

- Both video and audio streams delivered over wired Ethernet, when connected

Pros/Cons of Session Layer Control

Pro: Per-session control over mobility

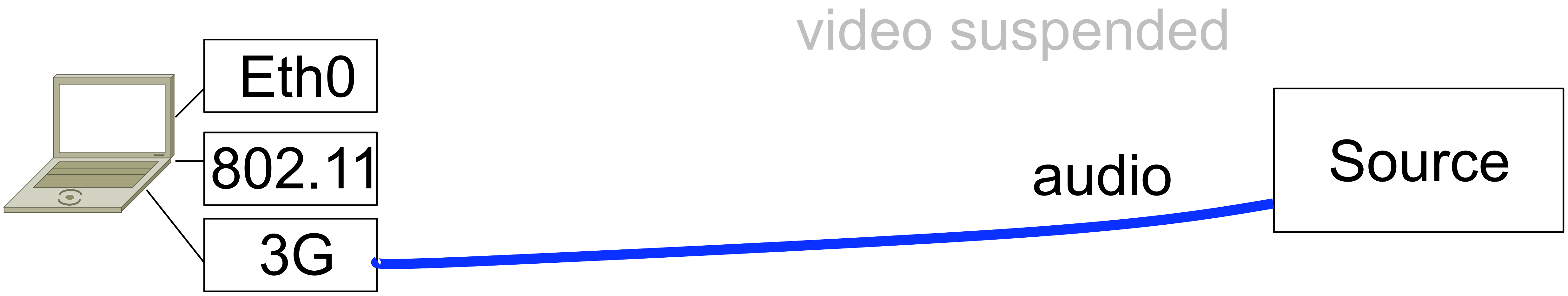


User unplugs, and moves through a 802.11 hot-spot

- Video delivered over 802.11
- Audio delivered over 3G wireless

Pros/Cons of Session Layer Control

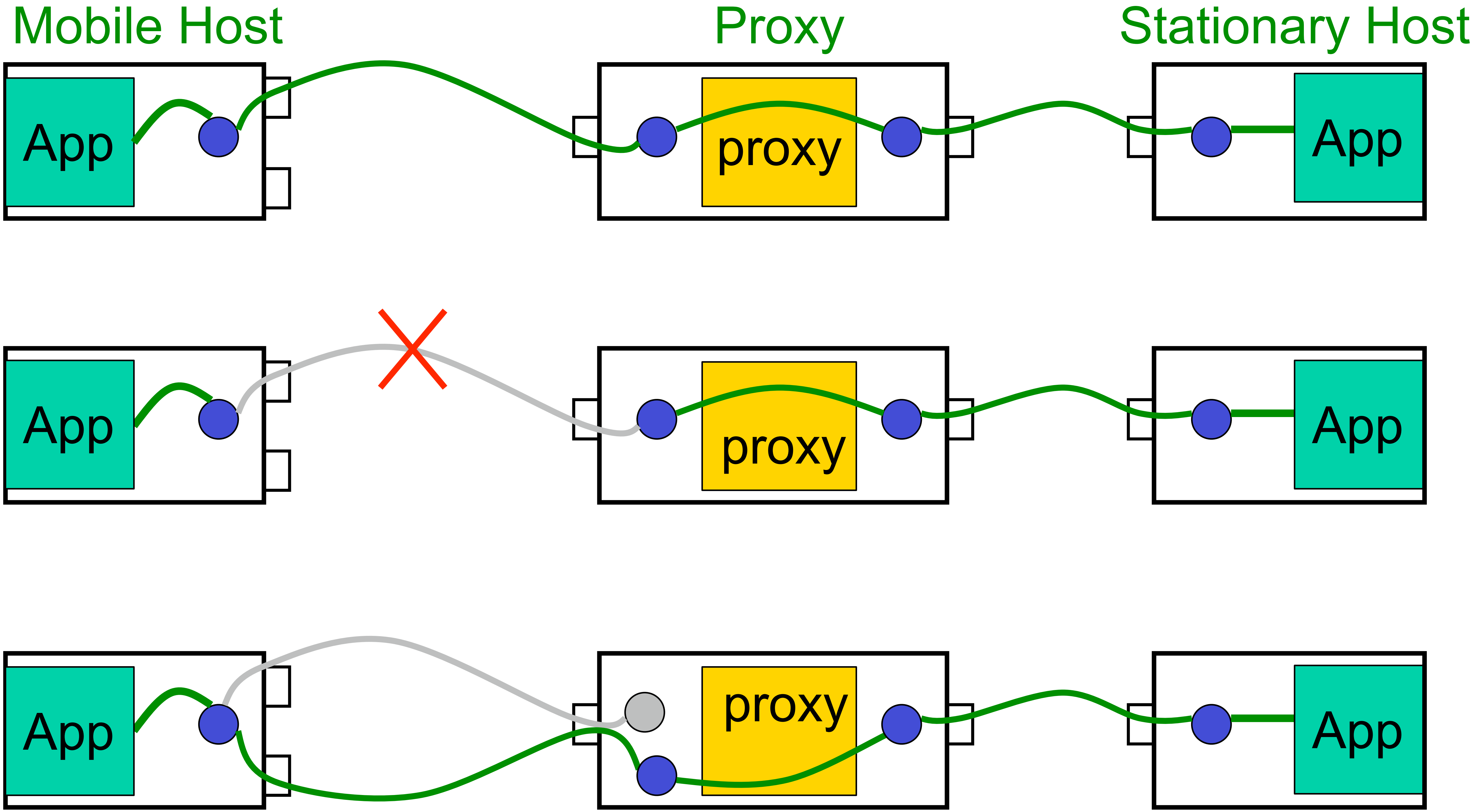
Pro: Per-session control over mobility



User leaves 802.11 hot-spot, or signal is marginal

- Video stream suspended
- Audio continues over 3G wireless

MSOCKS


Mobile Host
Proxy
Stationary Host
App
proxy
App
App
proxy
App
App
proxy
App

Pros/Cons of MSOCKS

Pro: Completely backwards compatible

- No changes to stationary host
- Proxy hides all mobility issues
- Only shared library upgrade on mobile host

Pro: Proxy can perform ***transcoding*** as needed

- Compression, reformatting images, etc.
- Policy per mobile host, per session

Con: All traffic goes through proxy (triangle routing)

- Same as Mobile IP with reverse tunnels

Classic Problem with Session Approaches

Application sends its IP address to remote host, ***then relocates and changes its address***

- Example msg: “contact me at addr 1.1.1.1”
- Remote host has no way to find new IP addr
- Problem for FTP, callbacks, some P2P, …

“Solutions” – neither is perfect

- Forbid application to send an IP address – must send DNS name (Migrate)
- Trick application into providing address of a stationary socket (MSOCKs)

Other Concerns with Session Layer Mobility

Must solve the same problem multiple times

- Each Transport/Session layer must have mobility added
- TCP, UDP, RTP, …

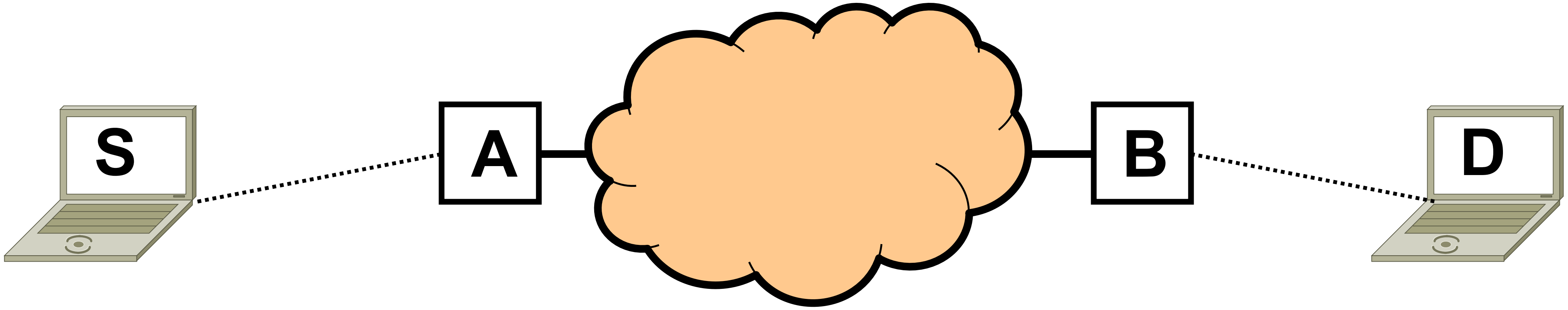
DNS servers make bad location registries

- Records for frequently moving hosts should not be cached by other DNS servers
- Yet, they will be: 20% of DNS servers cache data longer than they should [Pang, IMC'04]

Challenge 1:
Coping with Indirect Communication

IP (and its mobility solutions) assume dst is reachable

- Network carries packets from src ***directly*** to dst



- What if S and D are never connected at same time?

Need message forwarding, not packet forwarding

- Email
- Data replication (PDA HotSync, Bayou, Lotus Notes)
- Delay tolerant networking

Should IP architecture supply persistence semantics?

Challenge 2: Coping with Bad Coverage

There will always be places with no- or low- connectivity

- Requires cross-layer optimization/interaction
- Suspend/resume in network stack insufficient
- Application ***must*** be involved

Potential solutions:

- Coda/Odyssey filesystem
- Disconnected operation
- Weakly connected operation

What are the right services and interfaces to support mobile apps?

Discussion

- Broadcasted over the Internet
- Please use the microphone